arXiv:0912.4854v2 [math.NT] 21 May 2010

THE EULER SYSTEM OF CYCLOTOMIC UNITS AND HIGHER FITTING IDEALS

TATSUYA OHSHITA

Abstract. Kurihara established a refinement of the minus-part of the Iwasawa main conjecture for totally real number fields using the higher Fitting ideals ([Ku]). In this paper, we study the higher Fitting ideals of the plus-part of the Iwasawa module associated to the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\mu_p)$ for an odd prime number p by similar methods as in [Ku]. We define *the higher cyclotomic ideals* $\{\mathfrak{C}_i\}_{i\geq 0}$, which are ideals of the Iwasawa algebra defined by the Kolyvagin derivatives of cyclotomic units, and prove that they give upper bounds of the higher Fitting ideals. Our result can be regarded as a refinement of the plus-part of the Iwasawa main conjecture for $\mathbb{Q}$.

1. Introduction

The Iwasawa main conjecture describes the characteristic ideals of certain Iwasawa modules. The characteristic ideals give various important knowledge on the structure of finitely generated torsion Iwasawa modules, but these are not enough to determine the pseudo-isomorphism classes of them (cf. §2) completely. The pseudo-isomorphism classes of finitely generated torsion Iwasawa modules are determined by the Fitting ideals. In [Ku], Kurihara proved that all the higher Fitting ideals of the minus-part of the Iwasawa modules associated to the cyclotomic $\mathbb{Z}_p$-extension of certain CM-fields coincide with the higher Stickelberger ideals, which are defined by analytic objects arising from p-adic L-functions (cf. [Ku] Theorem 1.1). His result is a refinement of the minus-part of the Iwasawa main conjecture for totally real number fields.

In this paper, we study the plus-part of the Iwasawa modules by similar methods as in [Ku]. We obtain upper bounds of the higher Fitting ideals of the Iwasawa modules. The main tool in [Ku] is the Kolyvagin system of Gauss sums. Instead, in this paper, we use the Euler system of cyclotomic units, so we can only treat the Iwasawa modules associated to the cyclotomic $\mathbb{Z}_p$-extension of subfields of cyclotomic fields.

We shall state the main theorem of this paper. Fix an odd prime number p. Let μ_n be the group of all n-th roots of unity contained in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. For an integer m with $m \geq 0$, let F_m be the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\mu_{p^{m+1}})$. We denote the ring of integers of F_m by $\mathcal{O}_{F_m}$, and the (unique) prime of $\mathcal{O}_{F_m}$ above p by $\mathfrak{p}_m$. We put $F_\infty := \bigcup_{m\geq 0} F_m$, and $\Gamma_m := \mathrm{Gal}(F_\infty/F_m)$ for any $m \geq 0$. Let $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_m/\mathbb{Q})]$. We define a Λ-module $X := \varprojlim A_m$, where A_m is the p-Sylow subgroup of the ideal class group of F_m and

Date: May 24, 2010.

the projective limit is taken with respect to the norm map. We say a Λ-module M is *pseudo-null* if its order is finite. Let X_{fin} be the largest pseudo-null Λ-submodule of X, and $X' := X/X_{\mathrm{fin}}$. We study X' instead of X by a technical reason (cf. Lemma 3.3).

Put $\Delta := \mathrm{Gal}(F_0/\mathbb{Q})$. Since $\mathrm{Gal}(F_\infty/\mathbb{Q}) \simeq \Delta \times \Gamma_0$ and the order of Δ is prime to p, we have a decomposition $\Lambda = \bigoplus_\chi \Lambda_\chi$, where χ runs through all characters in $\widehat{\Delta} := \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$, and Λ_χ is a $\mathbb{Z}_p$-algebra isomorphic to $\mathbb{Z}_p[[\Gamma_0]] \simeq \mathbb{Z}_p[[T]]$ on which Δ acts via χ. Then for any Λ-module M, we decompose $M = \bigoplus_\chi M_\chi$, where $M_\chi := M \otimes_\Lambda \Lambda_\chi$. Let $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})$ be the annihilator of $X_{\mathrm{fin},\chi}$ as a Λ_χ-module.

In this paper, we study the higher Fitting ideals $\{\mathrm{Fitt}_{\Lambda_\chi,i}(X'_\chi)\}_{i\geq 0}$ of X'_χ for a non-trivial character $\chi \in \widehat{\Delta}$. Note that X_χ and X'_χ belong to the same pseudo-isomorphism class, so the pseudo-isomorphism class of X_χ is determined by the family $\{\mathrm{Fitt}_{\Lambda_\chi,i}(X'_\chi)\}_{i\geq 0}$ (cf. Example 3.2).

In the case of the plus-part, a problem lies in how to define the ideals which are substitutes for the higher Stickelberger ideals because we do not have elements as the Stickelberger elements in group rings of Galois groups. We shall define an ideal $\mathfrak{C}_i$ of Λ, called *the higher cyclotomic ideals* $\mathfrak{C}_i$ for each $i \in \mathbb{Z}_{\geq 0}$ in §6, by using the Euler system of cyclotomic units (cf. Definition 6.6). Roughly speaking, first, we shall define the ideals $\mathfrak{C}_{i,F_m,N}$ of the group ring $R_{F_m,N} := \mathbb{Z}/p^N[\mathrm{Gal}(F_m/\mathbb{Q})]$ generated by images of certain Kolyvagin derivatives $\kappa_{m,N}(\xi)$ by *all* $R_{F_m,N}$*-homomorphisms* $F_m^\times/(F_m^\times)^{p^N} \longrightarrow R_{F_m,N}$, then we shall define $\mathfrak{C}_i$ by the projective limit of them.

The goal of this paper is to prove the following theorem.

Theorem 1.1. *Let $\chi \in \widehat{\Delta}$ be a non-trivial character.*

(1) $\mathfrak{C}_{0,\chi} \subseteq \mathrm{Fitt}_{\Lambda_\chi,0}(X'_\chi)$.
(2) $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})\,\mathrm{Fitt}_{\Lambda_\chi,i}(X'_\chi) \subseteq \mathfrak{C}_{i,\chi}$ *for* $i \geq 0$.

For the case of the trivial character, see Remark 7.7. By Theorem 1.1, for $i = 0$, we obtain both upper and lower bounds of $\mathrm{Fitt}_{\Lambda_\chi,0}(X'_\chi)$. Since "error terms" $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})$ is an ideal of Λ_χ whose index is finite, Theorem 1.1 for $i = 0$ determines the characteristic ideal of X'_χ, which is equal to the characteristic ideal of X_χ (cf. Remark 7.9). Therefore, our theorem can be regarded as a refinement of the Iwasawa main conjecture. We use the Iwasawa main conjecture in the proof, so we do not give a new proof of the Iwasawa main conjecture. On the other hand, for $i \geq 1$, we obtain only upper bounds of $\mathrm{Fitt}_{\Lambda_\chi,i}(X'_\chi)$.

Theorem 1.1 gives some knowledge on the structure of the "growing-part" X' along the cyclotomic $\mathbb{Z}_p$-extension of F_0. But it gives nothing on the pseudo-null-part X_{fin}. In particular, if the Greenberg conjecture holds (i.e. if X_χ is pseudo-null, for example, see [Gr] Conjecture 3.4), then our theorem says nothing.

Remark 1.2. At the end of introduction, we remark on the case of F_0. Rubin determined the structure of A_0 (cf. [Ru1], [Ru2] and [MR]). In our notation, Rubin's result implies that the ideals $\{\mathfrak{C}_{i,F_0,N}\}_{i\geq 0}$ give the structure of $A_{0,\chi}$. For detail, see Remark 6.11.

Notation. In this paper, we use the following notation.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. In this paper, an algebraic number field is a subfield of $\overline{\mathbb{Q}}$ which is a finite extension of $\mathbb{Q}$.

Let L/K be a finite Galois extension of algebraic number fields. Let λ be a prime ideal of K, and λ' a prime ideal of L above λ. We denote the completion of K at λ by K_λ. If λ is unramified in L/K, the geometric Frobenius at λ' is denoted by $(\lambda', L/K) \in \mathrm{Gal}(L/K)$. (Note that some authors use the inverse of our $(\lambda', L/K)$.)

We fix a family of embeddings $\{\ \ell_{\overline{\mathbb{Q}}} \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell\ \}_{\ell:\mathrm{prime}}$ satisfying a technical condition (A) as follows.

(A) For any subfield $K \subset \overline{\mathbb{Q}}$ which is a finite Galois extension of $\mathbb{Q}$ and any element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, there exist infinitely many prime numbers ℓ such that ℓ is unramified in $K/\mathbb{Q}$ and $(\ell_K, K/\mathbb{Q}) = \sigma$, where ℓ_K is the prime ideal corresponding to the embedding $\ell_{\overline{\mathbb{Q}}}|_K$.

We can prove the existence of a family satisfying the condition (A) by the Chebotarev density theorem easily.

Let ℓ be a prime number. For an algebraic number field K, let ℓ_K be the prime ideal of K corresponding to the embedding $\ell_{\overline{\mathbb{Q}}}|_K$. Then, if $K_1 \supseteq K_2$ is an extension of algebraic number fields, we have $\ell_{K_1}|\ell_{K_2}$.

For an abelian group M and a positive integer n, we write M/n in place of M/nM for simplicity. In particular, for the multiplicative group $K^\times$ of a field K, we write $K^\times/p^N$ in place of $K^\times/(K^\times)^{p^N}$.

For a Λ-module M, we denote the Γ_m-invariants (resp. Γ_m-coinvariants) of M by M^{Γ_m} (resp. M_{Γ_m}).

Let R be a commutative ring. For an R-module M, we define $\mathrm{ann}_R(M)$ to be annihilator of M. Namely,

$$\mathrm{ann}_R(M) := \{a \in R \mid am = 0 \text{ for any } m \in M\}.$$

Acknowledgement

The author would like to thank Professors Kazuya Kato, Masato Kurihara and Tetsushi Ito for their helpful advices. This work was supported by Grant-in-Aid for JSPS Fellows (22-2753) from Japan Society for the Promotion of Science.

2. Preliminaries

In this section, we recall some preliminary results used in this paper. We use the same notation as in §1. In particular, F_m is the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\mu_{p^{m+1}})$, and $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$.

2.1. Here, we briefly recall the plus-part of the Iwasawa main conjecture.

First, we recall the definition of the characteristic ideals. Let $\chi \in \widehat{\Delta}$ be a character. Two Λ_χ-modules M and N are said to be *pseudo-isomorphic* and we write $M \sim N$ if there is a Λ_χ-homomorphism $M \longrightarrow N$ whose kernel and cokernel are pseudo-null. The relation $\sim$ is an equivalence relation of finitely generated torsion Λ_χ-modules. For a finitely generated torsion Λ_χ-module M, there exists a finite sequence $f_1, f_2, \dots, f_n$ of non-zero elements of Λ_χ such that f_i divides f_{i+1} for $1 \leq i \leq n-1$ and $M \sim \bigoplus_{i=1}^n \Lambda_\chi/f_i\Lambda_\chi$. We define the characteristic ideal $\mathrm{char}_{\Lambda_\chi}(M)$ of M by

$$\mathrm{char}_{\Lambda_\chi}(M) := f_1 f_2 \cdots f_n \Lambda_\chi.$$

Note that characteristic ideals are well-defined and depend on the pseudo-isomorphism classes.

To state the Iwasawa main conjecture, we next recall some preliminary results on unit groups.

For a subgroup M of the unit group $\mathcal{O}_{F_m}^\times$, we define M^1 by

$$M^1 := \{a \in M \mid a \equiv 1 \pmod{\mathfrak{p}_m}\}.$$

When $M = \mathcal{O}_{F_m}^\times$, we write $\mathcal{O}_{F_m}^1$ in place of $(\mathcal{O}_{F_m}^\times)^1$.

We write $F_{\mathfrak{p}_m}$ for the completion of F_m at the place $\mathfrak{p}_m$. For a subset M of F_m, let $\overline{M}$ denote the closure of M in $F_{\mathfrak{p}_m}$. Let C_{F_m} be the group of cyclotomic units of F_m (cf. [CS] Definition 4.3.1 or [Wa] §8.1). We define

$$\overline{\mathcal{O}_\infty^1} := \varprojlim \overline{\mathcal{O}_{F_m}^1},$$

$$\overline{C_\infty^1} := \varprojlim \overline{C_{F_m}^1},$$

where the projective limit is taken with respect to the norm map.

Proposition 2.1. (1) *The Λ-module X is finitely generated torsion.*
(2) *The Λ-module $\overline{\mathcal{O}_\infty^1}$ is free of rank 1.*
(3) *The Λ-module $\overline{C_\infty^1}$ is free of rank 1.*

Proof. The first assertion is a special case of [Wa] Lemma 13.18. The second assertion is [CS] Theorem 4.7.1. For the last assertion, see the proof of [CS] Theorem 4.4.1. □

Note that by Proposition 2.1 (2) and (3), the χ-part $(\overline{\mathcal{O}_\infty^1}/\overline{C_\infty^1})_\chi = (\overline{\mathcal{O}_\infty^1})_\chi/(\overline{C_\infty^1})_\chi$ is a finitely generated torsion Λ_χ-module. Then, by the Proposition 2.1, we can consider $\mathrm{char}_{\Lambda_\chi}(X_\chi)$ and $\mathrm{char}_{\Lambda_\chi}\left((\overline{\mathcal{O}_\infty^1}/\overline{C_\infty^1})_\chi\right)$. The statement of the Iwasawa main conjecture is the following:

$$\mathrm{char}_{\Lambda_\chi}(X_\chi) = \mathrm{char}_{\Lambda_\chi}\left((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\right) \text{ for any character } \chi \in \widehat{\Delta}.$$

2.2. Here, we recall some results on Γ_m-coinvariants (or invariants) of certain Λ-modules. They play important roles in the technical aspects in this paper. In particular, we need them when we determine "error terms" in Theorem 1.1.

Proposition 2.2 (a special case of [Wa] Proposition 13.22)**.** *Let m be an integer with $m \geq 0$. Then, we have the canonical isomorphism*

$$X_{\Gamma_m} \simeq A_m.$$

For each $m \geq 0$, we define

$$N_\infty(\mathcal{O}^\times_{F_m}) := \bigcap_{n \geq m} N_{F_n/F_m}(\mathcal{O}^\times_{F_n}),$$
$$N_\infty(\mathcal{O}^1_{F_m}) := \bigcap_{n \geq m} N_{F_n/F_m}(\mathcal{O}^1_{F_n}),$$

and

$$N_\infty(\overline{\mathcal{O}^1_{F_m}}) := \bigcap_{n \geq m} N_{F_{\mathfrak{p}n}/F_{\mathfrak{p}m}}(\overline{\mathcal{O}^1_{F_n}}).$$

Note that we have $N_\infty(\overline{\mathcal{O}^1_{F_m}}) = \overline{N_\infty(\mathcal{O}^1_{F_m})}$.

Proposition 2.3. *Let m be an integer with $m \geq 0$.*

(1) *The canonical homomorphism* $\mathrm{pr}(m, C)\colon (\overline{C^1_\infty})_{\Gamma_m} \longrightarrow \overline{C^1_{F_m}}$ *is surjective. The kernel of* $\mathrm{pr}(m, C)$ *is isomorphic to $\mathbb{Z}_p$ with the trivial action of* $\mathrm{Gal}(F_\infty/\mathbb{Q})$*.* ([CS] Theorem 4.6.3.)
(2) *The image of the canonical homomorphism* $\mathrm{pr}(m, \mathcal{O}^1)\colon (\overline{\mathcal{O}^1_\infty})_{\Gamma_m} \longrightarrow \overline{\mathcal{O}^1_{F_m}}$ *is* $N_\infty(\overline{\mathcal{O}^1_{F_m}})$*. The kernel of* $\mathrm{pr}(m, \mathcal{O}^1)$ *is isomorphic to $\mathbb{Z}_p$ with the trivial action of* $\mathrm{Gal}(F_\infty/\mathbb{Q})$*.* ([CS] Theorem 4.7.4.)

The following corollary immediately follows from Proposition 2.3.

Corollary 2.4. *For all $m \geq 0$ and non-trivial character $\chi \in \widehat{\Delta}$, we have the following canonical isomorphisms of $\mathbb{Z}_p[\mathrm{Gal}(F_m/\mathbb{Q})]$-modules:*

(1) $(\overline{C^1_\infty})_{\Gamma_m,\chi} \simeq (\overline{C^1_{F_m}})_\chi$;
(2) $(\overline{\mathcal{O}^1_\infty})_{\Gamma_m,\chi} \simeq N_\infty(\overline{\mathcal{O}^1_{F_m}})_\chi$.

Proposition 2.5 ([CS] Theorem 4.7.6)**.** *For all $m \geq 0$, we have the canonical isomorphism of $\mathbb{Z}_p[\mathrm{Gal}(F_m/\mathbb{Q})]$-modules*

$$X^{\Gamma_m} \simeq \overline{\mathcal{O}^1_{F_m}}/N_\infty(\overline{\mathcal{O}^1_{F_m}}).$$

Corollary 2.6. *The Λ-module $\overline{\mathcal{O}^1_{F_m}}/N_\infty(\overline{\mathcal{O}^1_{F_m}})$ is annihilated by* $\mathrm{ann}_\Lambda(X_{\mathrm{fin}})$*.*

Proof of Corollary 2.6. Since X_{Γ_m} is isomorphic to the finite group A_m by Proposition 2.2, the Λ-module X^{Γ_m} is pseudo-null. Then, X^{Γ_m} is contained in X_{fin}. Hence Corollary 2.6 follows from Proposition 2.5. □

Remark 2.7. By Leopoldt's conjecture for F_m (cf. [Wa] Corollary 5.32), we have the natural isomorphism

$$\mathcal{O}^1_{F_m} \otimes \mathbb{Z}_p \xrightarrow{\simeq} \overline{\mathcal{O}^1_{F_m}}.$$

Then, we have the following isomorphisms:

(1) $\mathcal{O}^\times_{F_m} \otimes \mathbb{Z}_p \xleftarrow{\simeq} \mathcal{O}^1_{F_m} \otimes \mathbb{Z}_p \xrightarrow{\simeq} \overline{\mathcal{O}^1_{F_m}}$;

(2) $N_\infty(\mathcal{O}^\times_{F_m}) \otimes \mathbb{Z}_p \xleftarrow{\simeq} N_\infty(\mathcal{O}^1_{F_m}) \otimes \mathbb{Z}_p \xrightarrow{\simeq} N_\infty(\overline{\mathcal{O}^1_{F_m}})$;

(3) $C^\times_{F_m} \otimes \mathbb{Z}_p \xleftarrow{\simeq} C^1 \otimes \mathbb{Z}_p \xrightarrow{\simeq} \overline{C^1_{F_m}}$.

3. Fitting ideals

Here, we recall the notion of higher Fitting ideals.

Definition 3.1 (Higher Fitting ideals, see [No] §3.1)**.** Let R be an commutative ring, and M be a finitely presented R-module. Let

$$R^m \xrightarrow{f} R^n \longrightarrow M \longrightarrow 0$$

be an exact sequence of R-modules. For each $i \geq 0$, we define *the i-th Fitting ideal* $\mathrm{Fitt}_{R,i}(M)$ as follows. When $0 \leq i < n$ and $m \geq n - i$, we define $\mathrm{Fitt}_{R,i}(M)$ to be the ideal of R generated by all $(n-i) \times (n-i)$ minors of the matrix corresponding to f. When $0 \leq i < n$ and $m < n - i$, we define $\mathrm{Fitt}_{R,i}(M) := 0$. When $i \geq n$, we define $\mathrm{Fitt}_{R,i}(M) := R$. The definition of these ideals depends only on M, and does not depend on the choice of the above exact sequence.

For a finitely presented R-module M, we have the following sequence of ideals of R:

$$\mathrm{Fitt}_{R,0}(M) \subseteq \mathrm{Fitt}_{R,1}(M) \subseteq \cdots \subseteq \mathrm{Fitt}_{R,n}(M) = \mathrm{Fitt}_{R,n+1}(M) = \cdots = R.$$

We denote the smallest number of generators of an R-module M by $\nu_R(M)$. If $\mathrm{Fitt}_{R,n}(M) \neq R$, then $\nu_R(M) \geq n+1$. Note that when R is a local ring or PID, we have $\nu_R(M) = i+1$ if and only if $\mathrm{Fitt}_{R,i}(M) \neq R$ and $\mathrm{Fitt}_{R,i+1}(M) = R$.

Example 3.2. Let $R = \mathbb{Z}_p[[T]]$ and M a finitely generated torsion R-module. Assume

$$M \sim \bigoplus_{i=1}^{n} R/f_iR$$

and f_i divides f_{i+1} for $1 \leq i \leq n-1$. Then, for each i with $i \geq 0$, there exists an ideal I_i with finite index in R such that

$$\mathrm{Fitt}_{R,i}(M) = \begin{cases} (\prod_{k=1}^{n-i} f_k) I_i & (\text{if } i < n) \\ I_i & (\text{if } i \geq n) \end{cases}$$

(cf. [Ku] Lemma 8.2). This implies that the family $\{\mathrm{Fitt}_{R,i}(M)\}_{i\geq 0}$ of Fitting ideals of M determines the pseudo-isomorphism class of M.

We need the following lemma in the proof of Theorem 1.1.

Lemma 3.3 (for example, see [Ku] Theorem 8.1)**.** *Let $R=\mathbb{Z}_p[[T]]$ and M a finitely generated torsion R-module. Suppose M contains no non-trivial pseudo-null R-submodule. Then, there exists an exact sequence*

$$0 \longrightarrow R^n \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

for some integer $n>0$, and we have

$$\mathrm{Fitt}_{R,0}(M)=\mathrm{char}_R(M).$$

4. The Euler system of cyclotomic units

We first recall some basic results on the Euler system of cyclotomic units in §§4.1-4.3. Then, in §4.4, we define Kurihara's elements $x_{\nu,q}\in(F_m^\times/p^N)_\chi$, which play a key role in the proof of Theorem 1.1 (cf. Definition 4.16).

4.1. We fix a primitive p^{m+1}-st root of unity $\rho_m\in\mathbb{Q}(\mu_{p^{m+1}})$ for each $m\geq 0$ such that $\rho_{m+1}^p=\rho_m$, and a topological generator $e\in\mathbb{Z}_{>0}$ of $\mathbb{Z}_p^\times$. We have the following lemma.

Lemma 4.1 ([Wa] Lemma 8.1)**.** *We define the element* $\mathrm{cyc}(\rho_m)$ *of C_{F_m} by*

$$\mathrm{cyc}(\rho_m):=\frac{\rho_m^{-e/2}-\rho_m^{e/2}}{\rho_m^{-1/2}-\rho_m^{1/2}}.$$

Then, the $\mathbb{Z}[\mathrm{Gal}(F_m/\mathbb{Q})]$-module C_{F_m} is generated by $\pm\mathrm{cyc}(\rho_m)$*.*

Corollary 4.2 ([CS] Lemma 4.3.4)**.** *The Λ-module $\overline{C^1_\infty}$ is generated by $\big(u{\cdot}\mathrm{cyc}(\rho_m)\big)_{m\geq 0}$, where u is a $(p-1)$-st root of unity in $\mathbb{Q}_p$ such that $eu\equiv 1 \pmod p$.*

For an integer $N\geq 1$, we define

$$\begin{aligned}\mathcal{S}_N &:= \big\{\ell \mid \ell \text{ is a prime number not dividing } e, \text{ and } \ell\equiv 1 \pmod{p^N}\big\},\\ \mathcal{N}_N &:= \Big\{\prod_{i=1}^r \ell_i \mid r>0,\ \ell_i\in\mathcal{S}_N\ (i=1,\dots,r),\text{ and } \ell_i\neq\ell_j \text{ if } i\neq j\Big\}\cup\{1\},\end{aligned}$$

and for any algebraic number field K, we define

$$\begin{aligned}\mathcal{S}_N(K) &:= \{\ell\in S_N \mid \ell \text{ splits completely in } K/\mathbb{Q}\},\\ \mathcal{N}_N(K) &:= \Big\{\prod_{i=1}^r \ell_i \mid r>0,\ \ell_i\in\mathcal{S}_N(K)\ (i=1,\dots,r),\text{ and } \ell_i\neq\ell_j \text{ if } i\neq j\Big\}\cup\{1\}.\end{aligned}$$

For $n=\prod_{i=1}^r\ell_i\in\mathcal{N}_N$ ($\ell_i\in\mathcal{S}_N$ for $i=1,\dots,r$), we define $\epsilon(n):=r$.

Definition 4.3. For $n \in \mathcal{N}_N$ and $\zeta \in \mu_{p^{m+1}n} \backslash \{1\}$, we define

$$\mathrm{cyc}(\zeta) := \frac{\zeta^{-e/2} - \zeta^{e/2}}{\zeta^{-1/2} - \zeta^{1/2}} \in F_m(n),$$

where $F_m(n)$ denotes the maximal totally real subfield of $\mathbb{Q}(\mu_{p^{m+1}n})$.

We obtain the following lemma immediately.

Lemma 4.4. *Let $n \in \mathcal{N}_N$.*

(1) *Let $\ell \in \mathcal{S}_N$, and assume ℓ does not divide n. Let $\zeta_\ell \in \mu_\ell$ be a primitive ℓ-th root of unity, and $\xi \in \mu_{p^{m+1}n} \backslash \{1\}$. Then*

$$N_{F_m(n\ell)/F_m(n)}\bigl(\mathrm{cyc}(\zeta_\ell \xi)\bigr) = \frac{\mathrm{cyc}(\xi^\ell)}{\mathrm{cyc}(\xi)}.$$

(2) *Let $\xi \in \mu_n$. Then*

$$N_{F_{m+1}(n)/F_m(n)}\bigl(\mathrm{cyc}(\rho_{m+1}\xi)\bigr) = \mathrm{cyc}(\rho_m \xi^p).$$

4.2. From now on, we assume $N \geq m+1$. Let $n \in \mathcal{N}_N$. In this subsection, we shall define an element $\kappa(\xi) \in F_m^\times/p^N$ called Kolyvagin derivative for any primitive $\xi \in \mu_n$. (In fact, we will define more general one. See Definition 4.8).

For an integer n prime to p, we write $n = \prod_{i=1}^r \ell_i^{e_i}$ such that $\ell_1, \dots, \ell_r$ are distinct prime numbers and $e_i > 0$ for each i. We define $F_m(n)$ to be the maximal totally real subfield of $\mathbb{Q}(\mu_{p^{m+1}n})$, and $H_{F_m,n} := \mathrm{Gal}\bigl(F_m(n)/F_m\bigr)$. Then, for any $m \geq 0$, we have canonical isomorphisms

$$\begin{aligned} H_{F_m,n} &= \mathrm{Gal}\bigl(F_m(n)/F_m\bigr) \simeq \mathrm{Gal}\bigl(\mathbb{Q}(\mu_{p^{m+1}n})/\mathbb{Q}(\mu_{p^{m+1}})\bigr) \\ &\simeq \mathrm{Gal}\bigl(\mathbb{Q}(\mu_n)/\mathbb{Q}\bigr) \\ &\simeq \mathrm{Gal}\bigl(\mathbb{Q}(\mu_{\ell_1}^{e_1})/\mathbb{Q}\bigr) \times \cdots \times \mathrm{Gal}\bigl(\mathbb{Q}(\mu_{\ell_r}^{e_r})/\mathbb{Q}\bigr) \\ &\simeq H_{\ell_1^{e_1}} \times \cdots \times H_{\ell_r^{e_r}}. \end{aligned}$$

For all m with $m \geq 0$, we identify $H_{F_m,n}$ with $H_{F_0,n}$ by canonical isomorphisms, and put $H_n := H_{F_0,n}$.

Recall H_ℓ is a cyclic group of order $\ell - 1$ if ℓ is a prime number. We shall take a generator σ_ℓ of H_ℓ for each prime number $\ell \in \mathcal{S}_N$ as follows. Let $\ell \in \mathcal{S}_N$. We put $N_{\{\ell\}} := \mathrm{ord}_p(\ell - 1)$, where ord_p is the normalized additive valuation of ℓ, namely, $\mathrm{ord}_p(p) = 1$. Then, we have $N_{\{\ell\}} \geq N \geq 1$. By the fixed embedding $\ell_{\overline{\mathbb{Q}}} \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, we regard $\mu_{p^{N_{\{\ell\}}}}$ as a subset of $\mathbb{Q}_\ell$. We identify $\mathrm{Gal}\bigl(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell\bigr)$ with $H_\ell = \mathrm{Gal}\bigl(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\bigr)$ by the canonical isomorphism. Let K be the maximal p-extension field of F_m contained in $F_m(\ell)$, and π the prime element of K_{ℓ_K}. We fix a generator σ_ℓ of H_ℓ such that

$$\pi^{\sigma_\ell - 1} \equiv \rho_{N_{\{\ell\}}-1} \pmod{\overline{\ell_K}},$$

where $\overline{\ell_K}$ is the maximal ideal of K_{ℓ_K}, and $\rho_{N_{\{\ell\}}-1}$ is a primitive $p^{N_{\{\ell\}}}$-th root of unity defined as above. Note that the definition of σ_ℓ does not depend on the choice of π.

Let $n \in \mathcal{N}_N$. We define the following elements of the group ring $\mathbb{Z}[H_n]$.

Definition 4.5. Let $n = \prod_{i=1}^{r} \ell_i \in \mathcal{N}_N$ such that $\ell_i \in \mathcal{S}_N$ for $i = 1, \dots, r$. We define

$$D_{\ell_i} := \sum_{k=1}^{\ell_i - 2} k\sigma_{\ell_i}^k \in \mathbb{Z}[H_{\ell_i}] \subseteq \mathbb{Z}[H_n]$$

for $i = 1, \dots, r$, and

$$D_n := \prod_{i=1}^{r} D_{\ell_i} \in \mathbb{Z}[H_n].$$

In order to define $\kappa(\xi)$, we need the following two well-known Lemmas.

Lemma 4.6. *Let $n_1, n_2 \in \mathcal{N}_N$ satisfying $(n_1, n_2) = 1$. We put $n = n_1 n_2$. Then, the canonical map $F_m(n_1)^\times/p^N \longrightarrow \big(F_m(n)^\times/p^N\big)^{H_{n_2}}$ is isomorphism.*

Lemma 4.7. *Let $n_1, n_2 \in \mathcal{N}_N$. Assume $\ell \in \mathcal{S}_N\big(F_m(n_1)\big)$ for each prime divisor ℓ of n_2. Namely, $\ell \equiv 1 \pmod{p^N n_1}$ for each prime divisor ℓ of n_2. We put $n = n_1 n_2$. Let $\xi_{n_1} \in \mu_{n_1}$ be a primitive n_1-st root of unity, and $\xi_{n_2} \in \mu_{n_2}$ a primitive n_2-nd root of unity. Then, the image of $\mathrm{cyc}(\rho_m \xi_{n_1} \xi_{n_2})^{D_{n_2}}$ in $F_m(n)^\times/p^N$ is fixed by $H_{n_2} = \mathrm{Gal}\big(F_m(n)/F_m(n_1)\big)$.*

Definition 4.8. Let $n_1, n_2 \in \mathcal{N}_N$. Assume $\ell \in \mathcal{S}_N\big(F_m(n_1)\big)$ for each prime divisor of n_2. We put $n = n_1 n_2$. Let $\xi \in \mu_n$ be a primitive n-th root of unity. We define

$$\kappa_{m,N}^{n_1}(\xi) \in F_m(n_1)^\times/p^N$$

to be the unique element of $F_m(n_1)^\times/p^N$ such that its image in $F_m(n)^\times/p^N$ is the class of $\mathrm{cyc}(\rho_m\xi)^{D_{n_2}}$. When no confusion arises, we denote $\kappa_{m,N}^{n_1}(\xi)$ by $\kappa^{n_1}(\xi)$ for simplicity.

When $n_1 = 1$, the element $\kappa^1(\xi) \in F_m^\times/p^N$ is denoted by $\kappa(\xi)$.

4.3. Let $R_{F_m,N} := \mathbb{Z}/p^N[\mathrm{Gal}(F_m/\mathbb{Q})]$. Let $\chi \in \widehat{\Delta}$ be a character. We define $R_{F_m,N,\chi} := \mathbb{Z}/p^N[\mathrm{Gal}(F_m)/\mathbb{Q}]_\chi$ to be the χ-part of $R_{F_m,N}$. Namely, $R_{F_m,N,\chi}$ is the ring isomorphic to $\mathbb{Z}/p^N[\mathrm{Gal}(F_m/F_0)]$ on which Δ acts via χ. Obviously, we have

$$R_{F_m,N} = \Lambda_{\Gamma_m}/p^N, \quad R_{F_m,N,\chi} = \Lambda_{\chi,\Gamma_m}/p^N \quad \text{and} \quad R_{F_m,N} = \bigoplus_{\chi \in \widehat{\Delta}} R_{F_m,N,\chi},$$

where Λ_{Γ_m} (resp. Λ_{χ,Γ_m}) denotes the Γ_m-coinvariant of Λ (resp. Λ_χ). For a $R_{F_m,N}$-module M and an element $x \in M$, we denote the χ-component of x by $x_\chi \in M_\chi$.

As in [Ku] §2.3, in this subsection, we shall define two homomorphisms

$$[\cdot]_{F_m,N,\chi}^{\ell} \colon (F_m^\times/p^N)_\chi \longrightarrow R_{F_m,N,\chi}$$

for each $\ell \in \mathcal{S}_N$ (cf. Definition 4.9), and

$$\bar{\phi}_{F_m(n),N,\chi}^{\ell} \colon (F_m(n)^\times/p^N)_\chi \longrightarrow R_{F_m,N,\chi}[H_n]$$

for each $n \in \mathcal{N}_N$ and $\ell \in \mathcal{S}_N\big(F_m(n)\big)$ (cf. Definition 4.10). The homomorphism $[\cdot]_{F_m,N,\chi}^{\ell}$ is defined by the valuations of the places above ℓ, and $\bar{\phi}_{F_m(n),N,\chi}^{\ell}$ is defined by the local reciprocity maps.

First, we define $[\cdot]^{\ell}_{F_m,N,\chi}$. Let K be an algebraic number field. We define $\mathcal{I}_K$ to be the group of fractional ideals of K, and we write its group law additively. We define the homomorphism $(\cdot)_K\colon K^{\times} \longrightarrow \mathcal{I}_K$ by

$$(x)_K = \sum_{\lambda} \mathrm{ord}_{\lambda}(x)\lambda,$$

where λ runs through all prime ideals of K, and ord_{λ} is the normalized valuation of λ. For any prime number ℓ, we define $\mathcal{I}^{\ell}_K$ to be the subgroup of $\mathcal{I}_K$ generated by all prime ideals above ℓ. Then, we define $(\cdot)^{\ell}_K\colon K^{\times} \longrightarrow \mathcal{I}^{\ell}_K$ by

$$(x)^{\ell}_K = \sum_{\lambda \mid \ell} \mathrm{ord}_{\lambda}(x)\lambda.$$

Recall that we fix a family of embeddings $\{\, \ell_{\overline{\mathbb{Q}}}\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{\ell} \,\}_{\ell:\mathrm{prime}}$ (cf. §1 Notation), and we denote the ideal of K corresponding to the embedding $\ell_{\overline{\mathbb{Q}}}|_K$ by ℓ_K for each prime number ℓ and algebraic number field K. Assume $\ell \in \mathcal{S}_N(K)$ and $K/\mathbb{Q}$ is Galois extension. Then, $\mathcal{I}^{\ell}_K$ is a free $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-module generated by ℓ_K, and we identify $\mathcal{I}^{\ell}_K$ with $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ by the isomorphism $\iota\colon \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})] \xrightarrow{\simeq} \mathcal{I}^{\ell}_K$ defined by $x \longmapsto x \cdot \ell_K$ for $x \in \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$. The composition $K^{\times} \longrightarrow \mathcal{I}^{\ell}_K \xrightarrow{\iota^{-1}} \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ is also denoted by $(\cdot)^{\ell}_K$.

Definition 4.9. We define the $R_{F_m,N,\chi}$-homomorphism

$$[\cdot]_{F_m,N,\chi}\colon (F_m^{\times}/p^N)_{\chi} \longrightarrow (\mathcal{I}_{F_m}/p^N)_{\chi}$$

to be the homomorphism induced by $(\cdot)^{\ell}_{F_m}\colon F_m^{\times} \longrightarrow \mathcal{I}_{F_m}$.

Let $\ell \in \mathcal{S}_N$. We define the $R_{F_m,N,\chi}$-homomorphism

$$[\cdot]^{\ell}_{F_m,N,\chi}\colon (F_m^{\times}/p^N)_{\chi} \longrightarrow R_{F_m,N,\chi} = \mathbb{Z}/p^N[\mathrm{Gal}(F_m/\mathbb{Q})]_{\chi}$$

to be the homomorphism induced by $(\cdot)^{\ell}_{F_m}\colon F_m^{\times} \longrightarrow \mathbb{Z}[\mathrm{Gal}(F_m/\mathbb{Q})]$.

Second, we will define $\bar{\phi}^{\ell}_{F_m(n),N,\chi}$. Let $n \in \mathcal{N}_N$, and $\ell \in \mathcal{S}_N(F_m(n))$. Since we assume $N \geq m+1$, the prime number ℓ splits completely in $F_m(n)/\mathbb{Q}$, and we have $F_m(n)_{\lambda} = \mathbb{Q}_{\ell}$ for any prime ideal λ of $F_m(n)$ above ℓ. We regard the group $\mathbb{Q}_{\ell}^{\times}$ as a $\mathbb{Z}[\mathrm{Gal}(F_m/\mathbb{Q})]$-module with the trivial action of $\mathrm{Gal}(F_m/\mathbb{Q})$, and groups $\bigoplus_{\lambda\mid\ell} F_m(n)_{\lambda}^{\times}$ and $\bigoplus_{\lambda\mid\ell} H_{\ell}$ are regarded as $\mathbb{Z}[\mathrm{Gal}(F_m/\mathbb{Q})]$-modules by the identification

$$\bigoplus_{\lambda\mid\ell} F_m(n)_{\lambda}^{\times} = \mathcal{I}^{\ell}_{F_m(n)} \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell}^{\times} \quad \text{and} \quad \bigoplus_{\lambda\mid\ell} H_{\ell} = \mathcal{I}^{\ell}_{F_m(n)} \otimes H_{\ell},$$

respectively.

We denote by

$$\phi_{\mathbb{Q}_{\ell}}\colon \mathbb{Q}_{\ell}^{\times} \longrightarrow \mathrm{Gal}\big(\mathbb{Q}_{\ell}(\mu_{\ell})/\mathbb{Q}_{\ell}\big) = \mathrm{Gal}\big(\mathbb{Q}(\mu_{\ell})/\mathbb{Q}\big) = H_{\ell}$$

the reciprocity map of local class field theory defined by $\phi_{\mathbb{Q}_\ell}(\ell) = (\ell_{\mathbb{Q}(\mu_\ell)}, \mathbb{Q}(\mu_\ell)/\mathbb{Q})$. The homomorphism

$$\phi^{\ell}_{F_m(n)} \colon F_m(n)^\times \longrightarrow \mathbb{Z}[\mathrm{Gal}(F_m(n)/\mathbb{Q})] \otimes H_\ell$$

is defined to be the composition of the three homomorphisms of $\mathbb{Z}[\mathrm{Gal}(F_m(n)/\mathbb{Q})]$-modules:

$$\mathrm{diag}\colon F_m(n)^\times \longrightarrow \textstyle\bigoplus_{\lambda|\ell} F_m(n)^\times_\lambda,$$

$$\oplus\phi_{\mathbb{Q}_\ell}\colon \textstyle\bigoplus_{\lambda|\ell} F_m(n)^\times_\lambda \longrightarrow \textstyle\bigoplus_{\lambda|\ell} H_\ell,$$

$$\iota_H^{-1}\colon \textstyle\bigoplus_{\lambda|\ell} H_\ell \xrightarrow{\simeq} \mathbb{Z}[\mathrm{Gal}(F_m(n)/\mathbb{Q})] \otimes H_\ell,$$

which are defined as follows:

(1) the first homomorphism diag is the diagonal inclusion;
(2) the second homomorphism $\oplus\phi_{\mathbb{Q}_\ell}$ is the direct sum of the reciprocity maps;
(3) the third isomorphism ι_H^{-1} is the inverse of the isomorphism

$$\iota_H\colon \mathbb{Z}[\mathrm{Gal}(F_m(n)/\mathbb{Q})] \otimes H_\ell \xrightarrow{\simeq} \textstyle\bigoplus_{\lambda|\ell} H_\ell = \mathcal{I}^{\ell}_{F_m(n)} \otimes H_\ell,$$

which is induced by the above isomorphism

$$\iota\colon \mathbb{Z}[\mathrm{Gal}(F_m(n)/\mathbb{Q})] \xrightarrow{\simeq} \mathcal{I}^{\ell}_{F_m(n)}$$

given by $x \longmapsto x \cdot \ell_{F_m(n)}$.

Definition 4.10. Let $n \in \mathcal{N}_N$, and $\ell \in \mathcal{S}_N(F_m(n))$. We define

$$\phi^{\ell}_{F_m(n),N,\chi}\colon (F_m(n)^\times/p^N)_\chi \longrightarrow \mathbb{Z}/p^N[\mathrm{Gal}(F_m(n)/\mathbb{Q})]_\chi \otimes H_\ell$$

to be the homomorphism of $R_{F_m,N,\chi}[H_n]$-modules induced by $\phi^{\ell}_{F_m(n)}$. The choice of a generator σ_ℓ of H_ℓ induces the $R_{F_m,N,\chi}[H_n]$-homomorphism

$$\bar{\phi}^{\ell}_{F(n)_m,N,\chi}\colon (F(n)^\times_m/p^N)_\chi \longrightarrow \mathbb{Z}[\mathrm{Gal}(F_m(n)/\mathbb{Q})]_\chi = R_{F_m,N,\chi}[H_n]\ .$$

Next, we shall prove some formulas of the Euler system of cyclotomic units. We fix a primitive ℓ-th root of unity ξ_ℓ for each $\ell \in \mathcal{S}_N$. For each $n \in \mathcal{N}_N$, we define a primitive n-th root of unity by

$$\xi_n = \prod_{\substack{\ell \in \mathcal{S}_N \\ \ell | n}} \xi_\ell.$$

As in [Ku], we use the notion *well-ordered*.

Definition 4.11. Let $n \in \mathcal{N}_N$. We call n *well-ordered* if and only if n has a factorization $n = \prod_{i=1}^{r} \ell_i$ such that $\ell_{i+1} \in S(F_m(\prod_{j=1}^{i} \ell_j))$ for$i = 1, \ldots, r$. In other words, n is well-ordered if and only if n has a factorization $n = \prod_{i=1}^{r} \ell_i$ such that

$$\ell_{i+1} \equiv 1 \pmod{p^N \prod_{j=1}^{i} \ell_j}$$

for $i = 1, \ldots, r-1$.

Proposition 4.12. *Let n be an integer contained in $\mathcal{N}_N$.*

(1) *If λ is a prime ideal of K not dividing n, the λ-component of $[\kappa(\xi_n)_\chi]_{F_m,N,\chi}$ is 0. In particular, if $q \in \mathcal{S}_N$ is a prime number not dividing n, we have*
$$[\kappa(\xi_n)_\chi]^q_{F_m,N,\chi} = 0.$$
(2) *Let ℓ be a prime number dividing n. Then,*
$$[\kappa(\xi_n)_\chi]^\ell_{F_m,N,\chi} = -\bar{\phi}^\ell_{F_m,N,\chi}(\kappa(\xi_{n/\ell})_\chi).$$
(3) *If n is well-ordered, then*
$$\bar{\phi}^\ell_{F_m,N,\chi}(\kappa(\xi_n)_\chi) = 0$$
for each prime number ℓ dividing n. (See [MR] Theorem A.4.)

Remark 4.13. The third assertion of Proposition 4.12 is cyclotomic unit version of Lemma 5.3 in [Ku], and also a special case of [MR] Theorem A.4. In this paper, using the argument in [Ku], we shall directly give a proof of Proposition 4.12 (3).

Proof. Let us prove Proposition 4.12.

We prove the first assertion. If λ is a prime ideal of F_m not dividing pn, the λ-component of $[\kappa(\xi_n)_\chi]_{F_m,N,\chi}$ is 0 since $F_m(n)/F_m$ is unramified outside pn. Let $\mathfrak{p}_m$ be the (unique) prime ideal of F_m above p, and $\mathfrak{P}$ a prime ideal of $F_m(n)$ above $\mathfrak{p}_m$. The ramification index of $\mathfrak{P}/\mathfrak{p}$ is 2. Since $p \neq 2$, the $\mathfrak{p}_m$-component of $[\kappa(\xi_n)_\chi]_{F_m,N,\chi}$ is 0. The proof of the first assertion is complete.

The second assertions is [CS] Theorem 5.4.9. Note that $l_\ell := -\bar{\phi}^\ell_{F_m,N,\chi}$ is used in [CS] instead of our $\bar{\phi}^\ell_{F_m,N,\chi}$.

We shall prove the third assertion. Assume $n = \prod_{i=1}^r \ell_i \in \mathcal{N}_N$, where $\ell_1, \dots, \ell_r$ are distinct prime numbers, and $\ell_{i+1} \equiv 1 \pmod{p^N \prod_{j=1}^i \ell_j}$ for each $i = 1, \dots, r-1$. We put $n_1 := \prod_{j=1}^{i-1} \ell_j$. Note $\ell_1 \in \mathcal{S}_N(F_m(n))$. It is sufficient to prove the following claim.

Claim 4.14. $\bar{\phi}^{\ell_i}_{F_m(n_1),N,\chi}\big(\kappa^{n_1}(\xi_n)\big) = 0.$

Let λ be a prime ideal of $F_m(n_1)$ above ℓ_i, and λ' the prime of $F_m(n_1\ell_i)$ above λ. Let π' be a prime element of $F_m(n_1\ell_i)_{\lambda'}$. We take the prime element π of $F_m(n_1)_\lambda$ defined by
$$\pi := N_{F_m(n_1\ell_i)_{\lambda'}/F_m(n_1)_\lambda}(\pi').$$

We have a decomposition $F_m(n_1)^\times_\lambda/p^N = U \times P$ as a group, where U is the image of the unit group of $F_m(n_1\ell_i)_\lambda$ and P is the cyclic subgroup generated by the image of π. Both group U and P are cyclic groups of order p^N. The group U is generated by the image of a $p^{N_{\ell_i}}$-th root of unity in $F_m(n_1)_\lambda$.

Similarly, we have the decomposition $F_m(n_1\ell_i)^\times_{\lambda'}/p^N = U' \times P'$ as a group, where U' is the image of the unit group of $F_m(n_1\ell_i)_{\lambda'}$ and P' is the cyclic subgroup generated by the image of π'. Both group U' and P' are cyclic groups of order p^N with the action of H_{ℓ_i}.

We consider the homomorphism $\phi_{\mathbb{Q}_\ell,N}\colon F_m(n_1)_\lambda^\times/p^N = \mathbb{Q}_\ell^\times/p^N \longrightarrow H_\ell \otimes \mathbb{Z}/p^N\mathbb{Z}$ induced by $\phi_{\mathbb{Q}_\ell}$. By local class field theory, the kernel of $\phi_{\mathbb{Q}_\ell,N}$ is P. On the other hand, the kernel of the natural homomorphism $\iota\colon F_m(n_1)_\lambda^\times/p^N \longrightarrow F_m(n_1\ell_i)_{\lambda'}^\times/p^N$ is also P. Then, we have $\ker\phi_{\mathbb{Q}_\ell,N} = \ker\iota$.

We shall show that $\iota\big(\kappa^{n_1}(\xi_n)\big) = 1$. Let λ'' be a prime ideal of $F_m(n)$ above λ. Since $F_m(n)_{\lambda''}/F_m(n_1)_\lambda$ is unramified and $\mathrm{cyc}(\rho_m\xi_n)$ is a unit in $F_m(n)_{\lambda''}$, the element $\kappa^{n_1\ell_i}(\xi_n)$ is contained in U'. Then, the action of H_{ℓ_i} on $\kappa^{n_1\ell_i}(\xi_n)^{D_{\ell_i}} \in F_m(n_1\ell_i)_{\lambda'}/p^N$ is trivial, and we have

$$\begin{aligned}\iota\big(\kappa^{n_1}(\xi_n)\big) &= \kappa^{n_1\ell_i}(\xi_n)^{D_{\ell_i}}\\ &= \kappa^{n_1\ell_i}(\xi_n)^{\sum_{k=1}^{\ell_i-2} k\sigma_{\ell_i}^k}\\ &= \kappa^{n_1\ell_i}(\xi_n)^{(\ell_i-1)(\ell_i-2)/2}\\ &= 1\end{aligned}$$

in $F_m(n_1\ell_i)_{\lambda'}^\times/p^N$. The proof of Claim 4.14 and Proposition 4.12 (3) is complete. □

4.4. In this subsection, we will define the Kurihara's elements $x_{\nu,q} \in (F_m^\times/p^N)_\chi$ which become a key of the proof of Theorem 1.1.

Definition 4.15. Let $q\nu = q\prod_{i=1}^r \ell_i \in \mathcal{N}_N$, where $q, \ell_1, \dots, \ell_r$ are distinct prime numbers. For a positive integer d dividing ν, we define $\tilde{\kappa}_{d,q} \in (F_m^\times/p^N)_\chi \otimes (\bigotimes_{\ell|d} H_\ell)$ by

$$\tilde{\kappa}_{d,q} := \kappa(\xi_q \prod_{\ell|d} \xi_\ell)_\chi \otimes \big(\bigotimes_{\ell|d} \sigma_\ell\big).$$

Let $q\nu \in \mathcal{N}_N$ and assume $q\nu$ is *well-ordered*. Assume that for each prime number ℓ dividing ν, an element $a_\ell \in R_{F_m,N,\chi} \otimes H_\ell$ is given. Then, we have an element $\bar{a}_\ell \in R_{F_m,N,\chi}$ such that $a_\ell = \bar{a}_\ell \otimes \sigma_\ell$. Note that we will take $\{a_\ell\}_{\ell|\nu}$ explicitly later, but here, we take arbitrary one.

For a positive integer d dividing ν, we define the element a_d by

$$a_d := \bigotimes_{\ell|d} a_\ell \in R_{F_m,N,\chi} \otimes \big(\bigotimes_{\ell|d} H_\ell\big),$$

and the element $\bar{a}_d \in R_{F_m,N,\chi}$ by

$$a_d = \bar{a}_d \otimes \big(\bigotimes_{\ell|d} \sigma_\ell\big).$$

Note that we write the group law of $(F_m^\times/p^N)_\chi \otimes \big(\bigotimes_{\ell|d} H_\ell\big)$ multiplicatively.

Definition 4.16. We define the element $\tilde{x}_{\nu,q}$ by

$$\tilde{x}_{\nu,q} := \prod_{d|\nu} a_d \otimes \tilde{\kappa}_{\nu/d,q} \in (F_m^\times/p^N)_\chi \otimes \big(\bigotimes_{\ell|d} H_\ell\big).$$

Note that we naturally identify the $R_{F_m,N,\chi}$-module $(F_m^\times/p^N)_\chi \otimes \bigl(\bigotimes_{\ell|d} H_\ell\bigr)$ with

$$(F_m^\times/p^N)_\chi \otimes_{R_{F_m,N,\chi}} R_{F_m,N,\chi} \otimes \Bigl(\bigotimes_{\ell|d} H_\ell\Bigr).$$

The element $x_{\nu,q} \in (F_m^\times/p^N)_\chi$ is defined by

$$\tilde{x}_{\nu,q} = x_{\nu,q} \otimes \Bigl(\bigotimes_{\ell|\nu} \sigma_\ell\Bigr).$$

The following formulas follows from Proposition 4.12 easily.

Proposition 4.17 (cf. [Ku] Proposition 6.1)**.** *Let $q\nu \in \mathcal{N}_N$ and we assume that $q\nu$ is well-ordered.*

(1) *If λ is a prime ideal of K not dividing n, the λ-component of $[x_{\nu,q}]_{F_m,N,\chi}$ is* 0*. In particular, if s is a prime number not dividing $q\nu$, we have*

$$[x_{\nu,q}]^s_{F_m,N,\chi} = 0.$$

(2) *Let ℓ be a prime number dividing ν. Then, we have*

$$[x_{\nu,q}]^\ell_{F_m,N,\chi} = -\bar{\phi}^\ell_{F_m,N,\chi}(x_{\nu/\ell,q}).$$

(3) *Let ℓ be a prime number dividing ν. Then, we have*

$$\bar{\phi}^\ell_{F_m,N,\chi}(x_{\nu,q}) = \bar{a}_\ell \bar{\phi}^\ell_{F_m,N,\chi}(x_{\nu/\ell,q}).$$

5. An application of the Chebotarev density theorem

Recall that we fix a family of embeddings $\{\, \ell_{\overline{\mathbb{Q}}} \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell \,\}_{\ell:\text{prime}}$ satisfying the technical condition (A) for families of embeddings as follows.

(A) *For any subfield $K \subset \overline{\mathbb{Q}}$ which is a finite Galois extension of $\mathbb{Q}$ and any element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, there exist infinitely many prime numbers ℓ such that ℓ is unramified in $K/\mathbb{Q}$ and $(\ell_K, K/\mathbb{Q}) = \sigma$, where ℓ_K is the prime ideal of K corresponding to the embedding $\ell_{\overline{\mathbb{Q}}}|_K$.*

Note that the existence of such a family of embeddings follows from the Chebotarev density theorem. We need the condition (A) in the proof of Proposition 5.1.

Here, we shall prove Proposition 5.1, which is the key of induction argument in the proof of Theorem 1.1. This proposition corresponds to Lemma 9.1 in [Ku].

Proposition 5.1. *Let $\chi \in \widehat{\Delta}$ be a non-trivial character. Assume $qn = q\prod_{i=1}^r \ell_i \in \mathcal{N}_N$, where $q, \ell_1, \dots, \ell_r$ are prime numbers. Suppose the following are given:*

- *an element $\tau_i \in R_{F_m,N,\chi} \otimes H_{\ell_i}$ for each $i = 1, \dots, r$;*
- *a finite $R_{F_m,N,\chi}$-submodule W of $(F_m^\times/p^N)_\chi$;*
- *a $R_{F_m,N,\chi}$-homomorphism $\lambda \colon W \longrightarrow R_{F_m,N,\chi}$.*

Then, there exist infinitely many $q' \in \mathcal{S}_N(F_m(n))$ which have the following properties:

(1) *the class of q'_{F_m} in $A_{m,\chi}$ coincides with the class of q_{F_m};*
(2) *there exists an element $z \in (F_m^\times \otimes \mathbb{Z}_p)_\chi$ such that*

$$(z)_{F_m,\chi} = (q'_{F_m} - q_{F_m})_\chi \in \big(\mathcal{I}_{F_m} \otimes \mathbb{Z}_p\big)_\chi,$$

and

$$\phi^{\ell_i}_{F_m,N,\chi}(z) = \tau_i$$

for each $i = 1, \ldots, r$;
(3) *the group W is contained in the kernel of $[\cdot]^{q'}_{F_m,N,\chi}$, and*

$$\lambda(x) = \bar{\phi}^{q'}_{F_m,N,\chi}(x)$$

for any $x \in W$.

Proof. We shall prove Proposition 5.1 by four steps, using argument as in [Ku].

The first step. Here, we first define a field $F_m\{n\}_\chi$, which is finite Galois over F_m. Then, we take an element $\sigma \in \mathrm{Gal}\big(K/\mathbb{Q}(\mu_{np^N})\big)$ corresponding to the conditions(1) and (2) of Proposition 5.1, where $K := F_m\{n\}_\chi \mathbb{Q}(\mu_{np^N})$ is the composition field.

Let v be a prime ideal of F_m. We denote the ring of integers of the completion $F_{m,v}$ of F_m at v by $\mathcal{O}_{F_{m,v}}$, and define the subgroup $\mathcal{O}^1_{F_{m,v}}$ of $\mathcal{O}^\times_{F_{m,v}}$ by

$$\mathcal{O}^1_{F_{m,v}} := \{x \mid x \equiv 1 \pmod{\bar{v}}\},$$

where $\bar{v}$ is the maximal ideal of $\mathcal{O}_{F_{m,v}}$. We denote the residue field of F_m at v by $k(v)$.

Let $F_m\{n\}$ be the maximal abelian p-extension of F_m unramified outside n. By global class field theory, we have the isomorphism

$$\frac{(\prod_{v|n} F^\times_{m,v}/\mathcal{O}^1_{F_{m,v}}) \times (\bigoplus_{u\nmid n} F^\times_{m,u}/\mathcal{O}^\times_{F_{m,u}})}{F_m^\times} \otimes \mathbb{Z}_p \xrightarrow{\simeq} \mathrm{Gal}\big(F_m\{n\}/F_m\big),$$

where u runs all finite places outside n. This isomorphism induces the homomorphism

$$\iota\colon \bigoplus_{v|n} k(v)^\times \otimes \mathbb{Z}_p \longrightarrow \mathrm{Gal}\big(F_m\{n\}/F_m\big).$$

Taking the χ-part, we obtain the homomorphism

$$\iota_\chi\colon \big(\bigoplus_{v|n} k(v)^\times \otimes \mathbb{Z}_p\big)_\chi \longrightarrow \mathrm{Gal}\big(F_m\{n\}/F_m\big)_\chi$$

of $\mathbb{Z}_p[\mathrm{Gal}(F_m/\mathbb{Q})]_\chi$-modules. We denote by $F_m\{n\}_\chi$ the intermediate field of $F_m\{n\}/F_m$ with $\mathrm{Gal}\big(F_m\{n\}_\chi/F_m\big) = \mathrm{Gal}(F_m\{n\}/F_m)_\chi$.

Recall $n = \prod_{i=1}^r \ell_i$, and all prime divisors ℓ_i of n split completely in $F_m/\mathbb{Q}$. By local Artin maps, we obtain the isomorphism

$$\big(\bigoplus_{v|n} k(v)^\times \otimes \mathbb{Z}_p\big)_\chi \xrightarrow{\simeq} \bigoplus_{1=1}^r \big(\mathbb{Z}_p[\mathrm{Gal}(F_m/\mathbb{Q})]_\chi \cdot \ell_{i,F_m}\big) \otimes H_{\ell_i},$$

and we identify them by this isomorphism. We take an element

$$\tau_\chi = (\tau_{\chi,v})_{v|n} \in \Big(\bigoplus_{v|n} k(v)^\times \otimes \mathbb{Z}_p\Big)_\chi$$

whose image in $\bigoplus_{1=1}^{r}(R_{F_m,N,\chi}\cdot \ell_{i,F_m})\otimes H_{\ell_i}$ is $(\tau_1\cdot \ell_{1,F_m},\dots,\tau_r\cdot \ell_{r,F_m})$.

Let $K := F_m\{n\}_\chi \mathbb{Q}(\mu_{p^N n})$ be the composition field. Since the subgroup Δ of $\mathrm{Gal}(F_m/\mathbb{Q})$ acts on $\mathrm{Gal}\big(F_m\{n\}_\chi/F_m\big)$ (resp. $\mathrm{Gal}\big(F_{N-1}(n)/F_m\big)$) via χ (resp. trivial character) and χ is non-trivial, we have

$$F_m\{n\}_\chi \cap \mathbb{Q}(\mu_{np^N}) = F_m\{n\}_\chi \cap F_{N-1}(n) = F_m.$$

Then, we take the element $\sigma\in \mathrm{Gal}\big(K/\mathbb{Q}(\mu_{np^N})\big)$ such that

$$\sigma|_{F_m\{n\}_\chi} = \iota_\chi(\tau_\chi)^{-1}(q_{F_m\{n\}_\chi}, F_m\{n\}_\chi/F_m).$$

The second step. Here, we shall take an element $\lambda'\in \mathrm{Gal}\big(L/\mathbb{Q}(\mu_{p^N})\big)$ corresponding to the condition (3) of Proposition 5.1, where L is the extension field of $\mathbb{Q}(\mu_{p^N})$ generated by all p^N-th roots of elements contained in W.

We define a projection $\mathrm{pr}\colon R_{F_m,N}\longrightarrow \mathbb{Z}/p^N\mathbb{Z}$ by

$$\sum_{g\in \mathrm{Gal}(F_m/\mathbb{Q})} a_g g \longmapsto a_1,$$

where $a_g\in \mathbb{Z}/p^N\mathbb{Z}$ for all $g\in \mathrm{Gal}(F_m/\mathbb{Q})$, and $1\in \mathrm{Gal}(F_m/\mathbb{Q})$ is the unit. We define $\lambda'\in \mathrm{Hom}(W,\mu_{p^N})$ by $x\longmapsto \rho_{N-1}^{\mathrm{pr}\circ\lambda(x)}$ for all $x\in W$. (Recall ρ_{N-1} is a primitive p^N-th root of unity defined in §4.1.) We use the following well-known lemma.

Lemma 5.2. *Let $P\colon \mathrm{Hom}_{R_{F_m,N,\chi}}(W, R_{F_m,N,\chi})\longrightarrow \mathrm{Hom}(W,\mathbb{Z}/p^N\mathbb{Z})$ be the map given by $f\longmapsto \mathrm{pr}\circ f$. Then, P is bijective.*

Indeed, the inverse of P is given by

$$h\longmapsto \left(x\longmapsto \sum_{g\in \mathrm{Gal}(F_m/\mathbb{Q})} h(g^{-1}x)g\right)\in \mathrm{Hom}_{R_{F_m,N,\chi}}(W,R_{F_m,N,\chi}),$$

for $h\in \mathrm{Hom}(W,\mathbb{Z}/p^N\mathbb{Z})$. Note that Δ acts on W via χ, so we have

$$\mathrm{Hom}_{R_{F_m,N}}(W,R_{F_m,N}) = \mathrm{Hom}_{R_{F_m,N,\chi}}(W,R_{F_m,N,\chi}).$$

The natural homomorphism

$$W\subset (F_m^\times/p^N)_\chi \longrightarrow \big(\mathbb{Q}(\mu_{p^N})^\times/p^N\ \big)_\chi$$

is injective since we have $H^1\big(\mathrm{Gal}\big(\mathbb{Q}(\mu_{p^N})/F_m\big),\mu_{p^N}\big)_\chi = 0$. So, we regard W as a subgroup of $\big(\mathbb{Q}(\mu_{p^N})^\times/p^N\big)_\chi$. Let L be the extension field of $\mathbb{Q}(\mu_{p^N})$ generated by all p^N-th roots of elements of $F_m^\times$ whose image in $F_m^\times/p^N$ is contained in W. We consider the Kummer pairing

$$\mathrm{Gal}\big(L/\mathbb{Q}(\mu_{p^N})\big)\times W\longrightarrow \mu_{p^N}.$$

This pairing induces the isomorphism $\mathrm{Hom}(W,\mu_{p^N})\simeq \mathrm{Gal}\big(L/\mathbb{Q}(\mu_{p^N})\big)$. We regard λ' as an element of $\mathrm{Gal}\big(L/\mathbb{Q}(\mu_{p^N})\big)$ by this isomorphism.

The third step. Here, we show that $K\cap L = \mathbb{Q}(\mu_{p^N})$.

Since we have the natural isomorphism

$$\mathrm{Gal}\left(\mathbb{Q}(\mu_{p^N})/\mathbb{Q}\right) \simeq \mathrm{Gal}\left(\mathbb{Q}(\mu_p)/\mathbb{Q}\right) \times \mathrm{Gal}\left(\mathbb{Q}(\mu_{p^N})/\mathbb{Q}(\mu_p)\right),$$

we regard $\mathrm{Gal}\left(\mathbb{Q}(\mu_p)/\mathbb{Q}\right)$ as a subgroup of $\mathrm{Gal}\left(\mathbb{Q}(\mu_{p^N})/\mathbb{Q}\right)$. Let $c \in \mathrm{Gal}\left(\mathbb{Q}(\mu_p)/\mathbb{Q}\right)$ be the complex conjugation. Namely, c is the unique element of $\mathrm{Gal}\left(\mathbb{Q}(\mu_{p^N})/\mathbb{Q}\right)$ of order 2. Since $KL/\mathbb{Q}(\mu_{p^N})$ is an abelian p-extension, we regard $\mathrm{Gal}\left(KL/\mathbb{Q}(\mu_{p^N})\right)$ as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^N})/\mathbb{Q})]$-module. We have a decomposition

$$\mathrm{Gal}\left(KL/\mathbb{Q}(\mu_{p^N})\right) = \mathrm{Gal}\left(KL/\mathbb{Q}(\mu_{p^N})\right)_+ \times \mathrm{Gal}\left(KL/\mathbb{Q}(\mu_{p^N})\right)_- \ ,$$

where $\mathrm{Gal}\left(KL/\mathbb{Q}(\mu_{p^N})\right)_+$ (resp. $\mathrm{Gal}\left(KL/\mathbb{Q}(\mu_{p^N})\right)_-$) denotes the subgroup of $\mathrm{Gal}\left(KL/\mathbb{Q}(\mu_{p^N})\right)$ on which c acts trivially (resp. by -1).

The element c acts on $\mathrm{Gal}\left(K/\mathbb{Q}(\mu_{p^N})\right)$ trivially since K is the extension field of $\mathbb{Q}(\mu_{p^N})$ generated by all elements of $F_m\{n\}_\chi F_m(n)$, which is totally real. On the other hand, The element c acts on $\mathrm{Gal}\left(L/\mathbb{Q}(\mu_{p^N})\right)$ by -1 since $\mathrm{Gal}\left(\mathbb{Q}(\mu_p)/\mathbb{Q}\right)$ acts on $\mathrm{Gal}\left(L/\mathbb{Q}(\mu_{p^N})\right)$ via the character $\chi^{-1}\omega$, where $\omega \in \mathrm{Hom}\left(\mathrm{Gal}\left(\mathbb{Q}(\mu_p)/\mathbb{Q}\right), \mu_{p-1}\right)$ is the Teichmüler character. Hence we have

$$K \cap L = \mathbb{Q}(\mu_{p^N}).$$

The fourth step. We shall complete the proof.

By the third step and the condition (A), there exists infinitely many prime numbers q' such that

$$\begin{cases} (q'_K, K/\mathbb{Q}) = \sigma \\ (q'_L, L/\mathbb{Q}) = \lambda'. \end{cases}$$

We shall prove that each of such q' unramified in $L/\mathbb{Q}$ satisfies conditions (1)-(3) of Proposition 5.1.

First, we show q' satisfies conditions (1) and (2). Let $\alpha = (\alpha_v)_v \in \mathbb{A}_{F_m}^\times$ be an idele whose q'_{F_m}-component is a prime element of $F_{m,q'_{F_m}}$, and other components are 1. Let $\beta = (\beta_v)_v \in \mathbb{A}_{F_m}^\times$ be an idele such that the q_{F_m}-component is a prime element of $F_{m,q_{F_m}}$, the $\prod_{v|n} F_{m,v}^\times$-component is $\tilde{\tau}_\chi^{-1}$ which is a lift of $\tau_\chi^{-1} \in \left(\prod_{v|n} k(v)^\times \otimes \mathbb{Z}_p\right)_\chi$ in $\prod_{v|n} \mathcal{O}_{F_{m,v}}^\times$, and other components are 1. By definition, ideles α and β have the same image in

$$\left(\frac{(\prod_{v|n} F_{m,v}^\times/\mathcal{O}_{F_{m,v}}^1) \times (\bigoplus_{u\nmid n} F_{m,u}^\times/\mathcal{O}_{F_{m,u}}^\times)}{F_m^\times} \otimes \mathbb{Z}_p\right)_\chi \simeq \mathrm{Gal}\left(F_m\{n\}_\chi/F_m\right).$$

This implies there exist $z \in (F_m^\times \otimes \mathbb{Z}_p)_\chi$ such that

$$\alpha = z\beta \ \text{ in } \left(((\prod_{v|n} F_{m,v}^\times/\mathcal{O}_{F_{m,v}}^1) \times (\bigoplus_{u\nmid n} F_{m,u}^\times/\mathcal{O}_{F_{m,u}}^\times)) \otimes \mathbb{Z}_p\right)_\chi.$$

Hence, we have $(z)_{F_m,\chi} = (q'_{F_m} - q_{F_m})_\chi$, and $\phi_{F_m,N,\chi}^{\ell_i}(z) = \tau_i$ for each $i = 1, \ldots, r$. The prime number q' satisfies conditions (1) and (2).

Next, we shall prove q' satisfies condition (3). Since q' is unramified in $L/\mathbb{Q}$, the group W is contained in the kernel of $[\cdot]^{q'}_{F_m,N,\chi}$. Since $(q'_L, L/\mathbb{Q}) = \lambda'$, for any $x \in W$, we have

$$\rho_{N-1}^{\mathrm{pro}\lambda(x)} = \lambda'(x) = (x^{1/p^N})^{\mathrm{Fr}_{q'}-1},$$

where $\mathrm{Fr}_{q'} \in \mathrm{Gal}(L/\mathbb{Q})$ is the arithmetic Frobenius at q', and $x^{1/p^N} \in L$ is a p^N-th root of x. Then, we obtain

$$\rho_{N-1}^{\mathrm{pro}\lambda(x)} \equiv x^{(q'-1)/p^N} \pmod{\overline{q'_M}}.$$

There is the (unique) intermediate field M of $F_m(q')/F_m$ whose degree over F_m is p^N since $q' \equiv 1 \pmod{p^N}$. Let π be the prime element of M_{N,q'_M}. By definition of $\sigma_{q'}$, we have

$$\pi^{\sigma_{q'}-1} \equiv \rho_{N-1} \pmod{\overline{q'_M}},$$

where $\overline{q'_M}$ is the maximal ideal of $M_{q'_M}$. Recall that W is contained in the kernel of $[\cdot]^{q'}_{F_m,N,\chi}$. By definition of $\bar{\phi}^{q'}_{F_m,N,\chi}$, we have

$$\pi^{\phi(x)-1} \equiv x^{(q'-1)/p^N} \pmod{\overline{q'_M}}$$

for all $x \in W$, where we put

$$\phi(x) := \sigma_{q'}^{\mathrm{pro}\bar{\phi}^{q'}_{F_m,N,\chi}(x)}.$$

Then, we have

$$x^{(q'-1)/p^N} \equiv \rho_{N-1}^{\mathrm{pro}\bar{\phi}^{q'}_{F_m,N,\chi}(x)} \pmod{\overline{q'_M}}$$

for all $x \in W$. Hence, we obtain

$$\rho_{N-1}^{\mathrm{pro}\lambda(x)} = \rho_{N-1}^{\mathrm{pro}\bar{\phi}^{q'}_{F_m,N,\chi}(x)}$$

for all $x \in W$. By Lemma 5.2, we have $\lambda = \bar{\phi}^{q'}_{F_m,N,\chi}|_W$. Therefore q' satisfies condition (3) of Proposition 5.1, and the proof is complete. □

6. The cyclotomic ideals

Here, we will define the i-th cyclotomic ideal $\mathfrak{C}_i$ of Λ for each $i \geq 0$ (cf. Definition 6.6). Recall we denote $\mathbb{Z}/p^N[\mathrm{Gal}(F_m/\mathbb{Q})]$ by $R_{F_m,N}$. First, we fix m and N.

Definition 6.1. For $n \in \mathcal{N}_N$, we define $W^n_{F_m,N}$ to be the $R_{F_m,N}$-submodule of $F_m^\times/p^N$ generated by $\{\kappa_{m,N}(\xi) \mid \xi \in \mu_n\}$.

Definition 6.2. Recall we put $\epsilon(n) := r$ for $n = \prod_{i=1}^r \ell_i \in \mathcal{N}_N$ ($\ell_i \in \mathcal{S}_N$ for $i = 1, \ldots, r$). We denote by $\mathfrak{C}_{i,F_m,N}$ the ideal of $R_{F_m,N}$ generated by images of all $R_{F_m,N}$-homomorphisms $f\colon W^n_{F_m,N} \longrightarrow R_{F_m,N}$, where n runs through all elements of $\mathcal{N}_N$ satisfying $\epsilon(n) \leq i$.

Remark 6.3. Since we have decomposition

$$\mathrm{Hom}_{R_{F_m,N}}(W^n_{F_m,N}, R_{F_m,N}) = \bigoplus_{\chi \in \widehat{\Delta}} \mathrm{Hom}_{R_{F_m,N,\chi}}(W^n_{F_m,N,\chi}, R_{F_m,N,\chi}),$$

the χ-part $\mathfrak{C}_{i,F_m,N,\chi}$ of $\mathfrak{C}_{i,F_m,N}$ coincides with the ideal generated by $\operatorname{Im} f_\chi$ of $R_{F_m,N,\chi}$, where f_χ runs through all elements of $\operatorname{Hom}_{R_{F_m,N,\chi}}(W^n_{F_m,N,\chi}, R_{F_m,N,\chi})$ for any $n \in \mathcal{N}_N$ with $\epsilon(n) \leq i$.

Then, we will define the i-th cyclotomic ideal $\mathfrak{C}_i$ by taking the projective limit of $\{\mathfrak{C}_{i,F_m,N}\}_{m,N}$. To define it, we need the following lemma.

Lemma 6.4. *Let m_1, m_2, N_1, N_2 be integers satisfying $N_1 \geq m_1 + 1$, $N_2 \geq m_2 + 1$, $m_2 \geq m_1$, and $N_2 \geq N_1$. The image of $\mathfrak{C}_{i,F_{m_2},N_2}$ in $R_{F_{m_1},N_1}$ by the natural surjection is contained in $\mathfrak{C}_{i,F_{m_1},N_1}$.*

Proof. It is sufficient to show the lemma in the following two cases:

(1) $(m_2, N_2) = (m_1, N_1 + 1)$;
(2) $(m_2, N_2) = (m_1 + 1, N_1)$.

In the case (1), our lemma is clear. We shall show the lemma in the case (2).

We put $m = m_1$, $N = N_1 = N_2$, $R_1 = R_{F_m,N}$, $R_2 = R_{F_{m+1},N}$, and the natural surjection $\mathrm{pr}\colon R_2 \longrightarrow R_1$. We show the following claim:

Claim 6.5. *For $f_2 \in \operatorname{Hom}_{R_2}(W^n_{F_{m+1},N}, R_2)$, there exists a homomorphism $f_1 \in \operatorname{Hom}_{R_2}(W^n_{F_{m+1},N}, R_1)$ such that* $\operatorname{Im} f_1 = \operatorname{Im}(\mathrm{pr} \circ f_2)$.

For each elements $\sigma \in \operatorname{Gal}(F_m/\mathbb{Q})$, we fix a lift $\bar{\sigma} \in \operatorname{Gal}(F_{m+1}/\mathbb{Q})$ of σ. We have

$$R_2^{\operatorname{Gal}(F_{m+1}/F_m)} = \{ \sum_{\sigma \in \operatorname{Gal}(F_m/\mathbb{Q})} a_\sigma \bar{\sigma} \mathbf{n} \mid a_\sigma \in \mathbb{Z}/p^N \},$$

where $\mathbf{n}$ is an element of R_2 defined by

$$\mathbf{n} := \sum_{\tau \in \operatorname{Gal}(F_{m+1}/F_m)} \tau.$$

We define the isomorphism $\varphi\colon R_2^{\operatorname{Gal}(F_{m+1}/F_m)} \longrightarrow R_1$ of R_1-modules by

$$\sum_{\sigma \in \operatorname{Gal}(F_m/\mathbb{Q})} a_\sigma \bar{\sigma} \mathbf{n} \longmapsto \sum_{\sigma \in \operatorname{Gal}(F_m/\mathbb{Q})} a_\sigma \sigma.$$

Let $\iota\colon F_m^\times/p^N \longrightarrow F_{m+1}^\times/p^N$ be the canonical homomorphism. Since F_m is totally real, the homomorphism ι is injective. We have

$$\mathrm{pr} \circ f_2 = \varphi \circ f_2 \circ \iota \circ N_{F_{m+1}/F_m},$$

where $N_{F_{m+1}/F_m}\colon F_{m+1}^\times/p^N \longrightarrow F_{m+1}^\times/p^N$ is induced by the norm map. Note that it follows from Lemma 4.4 that we have

$$N_{F_{m+1}/F_m}(W^1_{F_{m+1},N}) = W^1_{F_m,N}.$$

If we put $f_1 = \varphi \circ f_2 \circ \iota$, then we have

$$\operatorname{Im} f_1 = \operatorname{Im}(\mathrm{pr} \circ f_2).$$

Thus we have proved the claim. Our lemma follows from the claim immediately. □

Definition 6.6 (The i-th cyclotomic ideal)**.** We define *the i-th cyclotomic ideal* $\mathfrak{C}_i$ to be the ideal of Λ such that $\mathfrak{C}_i := \varprojlim \mathfrak{C}_{i,F_m,N}$, where the projective limit is taken with respect to the system of the natural homomorphisms $\mathfrak{C}_{i,F_{m_2},N_2} \longrightarrow \mathfrak{C}_{i,F_{m_1},N_1}$ for integers m_1, m_2, N_1, N_2 satisfying $N_1 \geq m_1 + 1$, $N_2 \geq m_2 + 1$, $m_2 \geq m_1$ and $N_2 \geq N_1$.

We shall prove Proposition 6.7, which is a proposition on the size of $\mathfrak{C}_0$.

Proposition 6.7. *Let χ be a non-trivial character in $\widehat{\Delta}$. Then,*

$$\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi}) \,\mathrm{char}_{\Lambda_\chi}\big((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\big) \subseteq \mathfrak{C}_{0,\chi} \subseteq \mathrm{char}_{\Lambda_\chi}\big((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\big).$$

Proof. First, we will prove that $\mathfrak{C}_{0,\chi}$ contains $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi}) \,\mathrm{char}_{\Lambda_\chi}\big((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\big)$ for a non-trivial character $\chi \in \widehat{\Delta}$. By Proposition 2.1 (2), we can take an isomorphism $\varphi\colon \overline{\mathcal{O}^1_\infty} \xrightarrow{\simeq} \Lambda$, and by Corollary 2.4, it induces an isomorphism

$$\bar{\varphi}_{F_m,N,\chi}\colon \big(N_\infty(\mathcal{O}^\times_{F_m})/p^N\big)_\chi = \big(N_\infty(\mathcal{O}^1_{F_m})/p^N\big)_\chi \xrightarrow{\simeq} R_{F_m,N,\chi}.$$

It follows from Corollary 4.2 that the image of $C^1_{F_m}$ in $F_m^\times/p^N$ coincides with $W^1_{F_m,N}$. It is sufficient to show that for any $\delta \in \mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})$,

$$\delta\bar{\varphi}_{F_m,N,\chi}\big(\text{the image of } (\overline{C^1_{F_m}})_\chi\big) \subseteq \psi(W^1_{F_m,N})$$

for a homomorphism $\psi \in \mathrm{Hom}_{R_{F_m,N,\chi}}(W^1_{F_m,N,\chi}, R_{F_m,N,\chi})$ since this means that the image of $\mathfrak{C}_{0,\chi}$ in $R_{F_m,N,\chi}$ contains the image of $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi}) \,\mathrm{char}_{\Lambda_\chi}\big((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\big)$ in $R_{F_m,N,\chi}$. We show a stronger assertion.

Claim 6.8. *Let $\mathcal{NO}_{F_m,N,\chi}$ be the image of the natural homomorphism*

$$\big(N_\infty(\mathcal{O}^\times_{F_m})/p^N\big)_\chi \longrightarrow \big(\mathcal{O}^\times_{F_m}/p^N\big)_\chi \subset \big(F_m^\times/p^N\big)_\chi.$$

There exists a homomorphism $\psi\colon \mathcal{NO}_{F,N} \longrightarrow R_{F_m,N}$ which makes the diagram

$$\begin{tikzcd}
\big(C^1_{F_m}/p^N\big)_\chi \arrow[r] \arrow[d] & \big(N_\infty(\mathcal{O}^1_{F_m})/p^N\big)_\chi \arrow[r, "\delta\bar{\varphi}_{F_m,N,\chi}"] \arrow[d] & R_{F_m,N,\chi} \\
W^1_{F_m,N,\chi} \arrow[r, hook] & (\mathcal{NO}_{F_m,N})_\chi \arrow[ur, dashed, "\psi"'] &
\end{tikzcd}$$

commute.

This claim immediately follows from the following lemma.

Lemma 6.9. *Let δ be an element of* $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})$*. For any homomorphism*

$$f\colon \big(N_\infty(\mathcal{O}^\times_{F_m})/p^N\big)_\chi \longrightarrow R_{F_m,N,\chi}$$

of $R_{F_m,N,\chi}$-modules, there exists a homomorphism $g\colon \mathcal{NO}_{F,N,\chi} \longrightarrow R_{F_m,N,\chi}$ which makes the diagram

$$\begin{tikzcd}
\big(N_\infty(\mathcal{O}^1_{F_m})/p^N\big)_\chi \arrow[r, "\delta f"] \arrow[d] & R_{F_m,N,\chi} \\
\mathcal{NO}_{F_m,N,\chi} \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

commute.

Proof of Lemma 6.9. We consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \big(N_\infty(\mathcal{O}^\times_{F_m}) \otimes \mathbb{Z}_p\big)_\chi \arrow[r] \arrow[d, "\times p^N"] & \big(\mathcal{O}^\times_{F_m} \otimes \mathbb{Z}_p\big)_\chi \arrow[r] \arrow[d, "\times p^N"] & \big((\mathcal{O}^\times_{F_m}/N_\infty(\mathcal{O}^\times_{F_m})) \otimes \mathbb{Z}_p\big)_\chi \arrow[r] \arrow[d, "\times p^N"] & 0 \\
0 \arrow[r] & \big(N_\infty(\mathcal{O}^\times_{F_m}) \otimes \mathbb{Z}_p\big)_\chi \arrow[r] & \big(\mathcal{O}^\times_{F_m} \otimes \mathbb{Z}_p\big)_\chi \arrow[r] & \big((\mathcal{O}^\times_{F_m}/N_\infty(\mathcal{O}^\times_{F_m})) \otimes \mathbb{Z}_p\big)_\chi \arrow[r] & 0,
\end{tikzcd}$$

where two rows are exact, and all vertical arrows $\times p^N$ are the homomorphisms taking p^N-th power. Applying the snake lemma, we find that the kernel of the natural homomorphism $\big(N_\infty(\mathcal{O}^\times_{F_m})/p^N\big)_\chi \longrightarrow (\mathcal{O}^\times_{F_m}/p^N)_\chi$ is a subquotient of the module

$$\big((\mathcal{O}^\times_{F_m}/N_\infty(\mathcal{O}^\times_{F_m})) \otimes \mathbb{Z}_p\big)_\chi \simeq \big(\overline{\mathcal{O}^1_{F_m}}/N_\infty(\overline{\mathcal{O}^1_{F_m}})\big)_\chi,$$

which is annihilated by δ by Corollary 2.6. This implies Lemma 6.9. □

Next, we will prove that $\mathfrak{C}_{0,\chi}$ is contained in $\mathrm{char}_{\Lambda_\chi}\big((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\big)$ for a non-trivial character $\chi \in \widehat{\Delta}$. Note that $R_{F_m,N,\chi}$ is an injective $R_{F_m,N,\chi}$-module since the $R_{F_m,N,\chi}$-module $\mathrm{Hom}_{\mathbb{Z}}(R_{F_m,N,\chi}, \mathbb{Q}/\mathbb{Z})$ is injective and free of rank 1. Let $f\colon W^1_{F_m,N,\chi} \longrightarrow R_{F_m,N,\chi}$ be an $R_{F_m,N,\chi}$- homomorphism. Since $R_{F_m,N,\chi}$ is an injective $R_{F_m,N,\chi}$-module, there exists a homomorphism $\tilde{f}\colon \big(\mathcal{O}^\times_{F_m}/p^N\big)_\chi \longrightarrow R_{F_m,N,\chi}$ whose restriction to $W^1_{F_m,N,\chi}$ coincides with f. Then, we have an element $a \in R_{F,N,\chi}$ which makes the following diagram

$$\begin{tikzcd}
\big(C^1_{F_m}/p^N\big)_\chi \arrow[r] \arrow[ddr] & \big(N_\infty(\mathcal{O}^1_{F_m})/p^N\big)_\chi \arrow[r, "\tilde{\varphi}_{F_m,N,\chi}", "\simeq"'] \arrow[d] & R_{F,N,\chi} \arrow[d, dotted, "\times a"] \\
& \big(\mathcal{O}^\times_{F_m}/p^N\big)_\chi \arrow[r, dashed, "\tilde{f}"] & R_{F,N,\chi} \\
& W^1_{F_m,N,\chi} \arrow[u, hook] \arrow[ur, "f"'] &
\end{tikzcd}$$

commute, where $\times a$ is the homomorphism multiplying a. This diagram implies that $f(W^1_{F_m,N,\chi})$ is contained in the image of $\mathrm{char}_{\Lambda_\chi}\big((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\big)$ in $R_{F_m,N,\chi}$. Therefore, we obtain $\mathfrak{C}_{0,\chi} \subseteq \mathrm{char}_{\Lambda_\chi}\big((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\big)$. □

Theorem 1.1 for $i = 0$ follows from Proposition 6.7 and the Iwasawa main conjecture.

Corollary 6.10 (Theorem 1.1 for $i = 0$)**.** *Let χ be a non-trivial character in $\widehat{\Delta}$.*

(1) $\mathfrak{C}_{0,\chi} \subseteq \mathrm{Fitt}_{\Lambda_\chi,0}(X'_\chi)$.
(2) $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})\,\mathrm{Fitt}_{\Lambda_\chi,0}(X'_\chi) \subseteq \mathfrak{C}_{0,\chi}$.

Note that Corollary 6.10 is a restatement of the Iwasawa main conjecture in terms of 0-th cyclotomic ideal. Indeed, we can obtain $\mathrm{char}_{\Lambda_\chi}(X_\chi)$ from this Corollary.

Remark 6.11. Here, we remark on the structure of A_0. Using the Kolyvagin derivatives and the Euler system arguments, Rubin determined the structure of A_0 completely. (See [Ru2] for the minus-part version of this result.) We can show that our $\mathfrak{C}_{i,F_0,N,\chi}$ is equal to the ideal of $R_{F_0,N,\chi}$ generated by $p^{\partial(i,N,\chi)}$, where $\partial(i,N,\chi)$ is the largest integer satisfying

$$\kappa_{0,N}(\xi_n)_\chi \in \left(\left(F_0^\times/(F_0^\times)^{p^N} \right)_\chi \right)^{p^{\partial(i,N,\chi)}}$$

for any n with $\epsilon(n) \leq i$. Hence, when $\chi \in \widehat{\Delta}$ is non-trivial and N is sufficiently large, Rubin's result can be described as

$$A_{0,\chi} \simeq \bigoplus_{i \geq 0} R_{F_0,N,\chi}/p^{\partial(i,N,\chi)-\partial(i+1,N,\chi)} \simeq \bigoplus_{i \geq 0} \mathfrak{C}_{i+1,F_0,N,\chi}/\mathfrak{C}_{i,F_0,N,\chi}$$

in our notation. Equivalently, we have $\mathrm{Fitt}_{R_{F_0,N,\chi},i}(A_0) = \mathfrak{C}_{i,F_0,N,\chi}$ for all $i \geq 0$, non-trivial $\chi \in \widehat{\Delta}$ and sufficiently large N. We also remark that Mazur and Rubin proved a general theorem in [MR] Theorem 4.5.9, which contains the above result as a special case.

7. Proof of the main theorem

In this section, we prove Theorem 1.1. Our argument is almost parallel to [Ku] §9, but we have to treat the pseudo-null-part X_{fin} of X and the unit group $\mathcal{O}_{F_m}^\times$ carefully.

First, we recall the notation and the statement of the theorem. The Λ-module X is defined by $X := \varprojlim A_m$, where A_m is the p-Sylow subgroup of the ideal class group of F_m and the projective limit is taken with respect to the norm map. The Λ-module X' is defined by $X' := X/X_{\mathrm{fin}}$, where X_{fin} is the maximal pseudo-null Λ-submodule of X. Our main theorem is as follows.

Theorem 7.1 (Theorem 1.1)**.** *Let χ be a non-trivial character in $\widehat{\Delta}$.*

(1) $\mathfrak{C}_{0,\chi} \subseteq \mathrm{Fitt}_{\Lambda_\chi,0}(X'_\chi)$.
(2) $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})\,\mathrm{Fitt}_{\Lambda_\chi,i}(X'_\chi) \subseteq \mathfrak{C}_{i,\chi}$ *for $i \geq 0$.*

We have already proved Theorem 1.1 for $i = 0$ in the last section. Here, we prove the second assertion for $i \geq 1$.

7.1. We spend this subsection on the setting of notations.

We assume that $\chi \in \widehat{\Delta}$ is non-trivial. Since X'_χ has no non-trivial pseudo-null submodules, we have an exact sequence

$$(1) \qquad \begin{tikzcd} 0 \arrow[r] & \Lambda_\chi^h \arrow[r, "f"] & \Lambda_\chi^h \arrow[r, "g"] & X'_\chi \arrow[r] & 0, \end{tikzcd}$$

by Lemma 3.3. Let M be the matrix corresponding to f with respect to the standard basis $(\mathbf{e}_i)_{i=1}^h$ of Λ_χ^h. Let $\{m_1, ..., m_h\}$ and $\{n_1, ..., n_h\}$ be permutations of $\{1, ..., h\}$. For any integer i satisfying $1 \leq i \leq h-1$, consider the matrix M_i which is obtained from M by eliminating the n_j-th rows ($j = 1, ..., i$) and the m_k-th columns ($k = 1, ..., i$). Here, we shall prove that $\delta \det M_i \in \mathfrak{C}_{i,\chi}$ for any $i \in \mathbb{Z}_{\geq 1}$ for any $\delta \in \operatorname{ann}(A_{\mathrm{fin}})$. If $\det M_i = 0$, this is trivial, so we assume that $\det M_i \neq 0$. If necessary, we permute $\{m_1, ..., m_i\}$, and assume $\det M_r \neq 0$ for all integers r satisfying $0 \leq r \leq i$.

For each $m \in \mathbb{Z}_{\geq 0}$, we take a positive integer N_m such that and $N_{m+1} > N_m > m+1$, and $p^{N_m} > \# A_m$ for any $m \in \mathbb{Z}_{\geq 0}$. For simplicity, we put $F := F_m$, $R := \mathbb{Z}_p[\mathrm{Gal}(F_m/F_0)]_\chi$, $N := N_m$ and $R_N := R_{F,N,\chi} = \mathbb{Z}/p^N[\mathrm{Gal}(F_m/F_0)]_\chi$. Let $A_{m,\mathrm{fin},\chi}$ be the image of $X_{\mathrm{fin},\chi}$ in $A_{m,\chi}$ by the natural homomorphism. By Proposition 2.2, the R-module $A'_{m,\chi} := X'_{\Gamma_m,\chi}$ is regarded as the quotient $A_{m,\chi}/A_{m,\mathrm{fin},\chi}$. From the exact sequence (1), we obtain the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R^h \arrow[r, "\bar{f}"] & R^h \arrow[r, "\bar{g}"] & A'_{m,\chi} \arrow[r] & 0, \end{tikzcd}$$

by taking the Γ_m-coinvariants.

The image of $\mathbf{e}_r$ in R^h is denoted by $\mathbf{e}_i^{(m)}$. We define $\mathbf{c}_1 := g(\mathbf{e}_1), \ldots, \mathbf{c}_h := g(\mathbf{e}_h)$, and $\mathbf{c}_r^{(m)}$ to be the image of $\mathbf{c}_r$ in $A_{m,\chi}/A_{m,\mathrm{fin},\chi}$, namely $\mathbf{c}_r^{(m)} := \bar{g}(\mathbf{e}_r^{(m)})$. We fix a lift $\tilde{\mathbf{c}}_r^{(m)} \in A_{m,\chi}$ of $\mathbf{c}_r^{(m)}$, and define

$$P_r := \{\ell \in \mathcal{S}_N \mid [\ell_F]_\chi = \tilde{\mathbf{c}}_r^{(m)}\},$$

where $[\ell_F]_\chi$ is the class of ℓ_F in $A_{m,\chi}$. We define $P := \bigcup_{r=1}^i P_r$, and P_F to be the set of all the prime ideals of F above P. Let J be the subgroup of $\mathcal{I}_F$ generated by P_F, and the R-submodule $\mathcal{F}$ of $(F^\times \otimes \mathbb{Z}_p)_\chi$ the inverse image of $(J \otimes \mathbb{Z}_p)_\chi$ by the homomorphism $(\cdot)_F \colon (F^\times \otimes \mathbb{Z}_p)_\chi \longrightarrow (\mathcal{I}_F \otimes \mathbb{Z}_p)_\chi$. We define a surjective homomorphism

$$\alpha \colon (J \otimes \mathbb{Z}_p)_\chi \longrightarrow R^h$$

by $\ell_F \mapsto \mathbf{e}_r$ for each $\ell \in P_r$ and r with $1 \leq r \leq h$. We define

$$\alpha_r := \mathrm{pr}_r \circ \alpha \colon \begin{tikzcd} (J \otimes \mathbb{Z}_p)_\chi \arrow[r, "\alpha"] & R^h \arrow[r, "\mathrm{pr}_r"] & R \end{tikzcd}$$

to be the composition of α and the r-th projection.

We define the homomorphism $\beta\colon \mathcal{F} \longrightarrow R^h$ to make the following diagram

$$\begin{tikzcd}[ampersand replacement=\&] \& \mathcal{F} \arrow[r, "(\cdot)_{F,\chi}"] \arrow[d, "\beta"] \& (J \otimes \mathbb{Z}_p)_\chi \arrow[r, two heads, "\text{can.}"] \arrow[d, "\alpha"] \& A'_{m,\chi} \arrow[d, equal] \& \\ 0 \arrow[r] \& R^h \arrow[r, "\bar{f}"] \& R^h \arrow[r, "\bar{g}"] \& A'_{m,\chi} \arrow[r] \& 0 \end{tikzcd} \tag{2}$$

commute, where can. is induced by the canonical homomorphism $J \longrightarrow A'_{m,\chi} = A_{m,\chi}/A_{m,\mathrm{fin},\chi}$. Note that since the second row of the diagram is exact, β is well-defined. We define

$$\beta_r := \mathrm{pr}_r \circ \beta\colon \mathcal{F} \xrightarrow{\beta} R^h \xrightarrow{\mathrm{pr}_r} R$$

to be the composition of β and the r-th projection.

We consider the diagram (2) by taking $(- \otimes \mathbb{Z}/p\mathbb{Z})$. First, we prove the following two lemmas, namely Lemma 7.2 and 7.3.

Lemma 7.2. *The canonical homomorphism $\mathcal{F}/p^N \longrightarrow (F^\times/p^N)_\chi$ is injective.*

Proof. Let x be an element in the kernel of the homomorphism $\mathcal{F}/p^N \longrightarrow (F^\times/p^N)_\chi$ and $\tilde{x}$ a lift of x in $\mathcal{F}$. Then, there exists $y \in (F^\times \otimes \mathbb{Z}_p)_\chi$ such that $\tilde{x} = y^{p^N}$. Since $(\tilde{x})_{F,\chi} \in (J \otimes \mathbb{Z}_p)_\chi$ and $(\mathcal{I}_F \otimes \mathbb{Z}_p)/(J \otimes \mathbb{Z}_p)$ is torsion free $\mathbb{Z}_p$-module, we have $(y)_{F,\chi} \in (J \otimes \mathbb{Z}_p)_\chi$. Hence, $y \in \mathcal{F}$, and we obtain $x = 1$. □

The R_N-module $\mathcal{F}/p^N$ is regarded as a submodule of $(F^\times/p^N)_\chi$ by Lemma 7.2.

We regard $(F^\times/p^N)_\chi$ as a Λ_χ-module. For an element $x \in (F^\times/p^N)_\chi$ and $\delta \in \mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})$, we denote the scaler multiple of x by $\delta \in \Lambda_\chi$ by x^δ.

Lemma 7.3. *Let $[\cdot]_{F,N,\chi}$ be the homomorphism $(F^\times/p^N)_\chi \longrightarrow (\mathcal{I}_F/p^N)_\chi$ induced by $(\cdot)_F\colon F^\times \longrightarrow \mathcal{I}_F$. Let x be an element of $(F^\times/p^N)_\chi$ such that $[x]_{F,N,\chi} \in (J/p^N)_\chi$. Then, for any $\delta \in \mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})$, x^δ is contained in $\mathcal{F}/p^N \subset (F^\times/p^N)_\chi$.*

Proof. Recall the canonical exact sequence:

$$0 \longrightarrow \mathcal{P} \longrightarrow \mathcal{I}_K \longrightarrow A_m \longrightarrow 0,$$

where $\mathcal{P}$ is defined by $\mathcal{P} = F^\times/\mathcal{O}_{F_m}^\times$. By the snake lemma for the commutative diagram

$$\begin{tikzcd}[ampersand replacement=\&] 0 \arrow[r] \& \mathcal{P} \arrow[r] \arrow[d, "\times p^N"] \& \mathcal{I}_F \arrow[r] \arrow[d, "\times p^N"] \& A_m \arrow[r] \arrow[d, "\times p^N"] \& 0 \\ 0 \arrow[r] \& \mathcal{P} \arrow[r] \& \mathcal{I}_F \arrow[r] \& A_m \arrow[r] \& 0, \end{tikzcd}$$

we obtain the following exact sequence

$$0 \longrightarrow A_m \longrightarrow \mathcal{P}/p^N \longrightarrow \mathcal{I}_K/p^N \longrightarrow A_m \longrightarrow 0. \quad (\text{Recall } p^{N_m} > \#A_m.)$$

Let B_m be the image of J in A_m, and $\mathcal{P}_0 = \mathcal{F}/\mathcal{O}_{F_m}^\times$. Then, we have the exact sequence

$$0 \longrightarrow \mathcal{P}_0 \longrightarrow J \longrightarrow B_m \longrightarrow 0,$$

and by a similar argument as above, we obtain the exact sequence

$$0 \longrightarrow B_m \longrightarrow \mathcal{P}_0/p^N \longrightarrow J/p^N \longrightarrow B_m \longrightarrow 0.$$

Now, we obtain the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & B_m \arrow[r] \arrow[d, hook] & \mathcal{P}_0/p^N \arrow[r] \arrow[d, hook] & J/p^N \arrow[r] \arrow[d, hook] & B_m \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & A_m \arrow[r] & \mathcal{P}/p^N \arrow[r] & \mathcal{I}_F/p^N \arrow[r] & A_m \arrow[r] & 0
\end{tikzcd} \tag{3}$$

whose two rows are exact, and the vertical arrows are injective. Since δA_m is contained in B_m, our lemma follows from a diagram chase. □

From the first row of the diagram (3), we obtain the following corollary immediately.

Corollary 7.4. *The order of the kernel of the homomorphism* $[\cdot]_{F,\chi} \colon \mathcal{F}/p^N \longrightarrow J/p^N$ *is finite.*

Let n be an element of $\mathcal{N}_N$ whose prime divisors are in P. We define P_F^n to be the set of all elements of P dividing n. We define J_n to be the subgroup of J generated by P_F^n, and the submodule $\mathcal{F}_{n,N}$ of $\mathcal{F}/p^N$ the inverse image of J_n by the restriction of $[\cdot]_{F,N,\chi}$ to $\mathcal{F}/p^N$. Note that $\mathcal{F}_{n,N}$ is a *finite* R_N-submodule of $(F^\times/p^N)_\chi$ by Corollary 7.4. We have obtained the following commutative diagram

$$\begin{tikzcd}
\mathcal{F}_{n,N} \arrow[r, "{[\cdot]_{F,\chi}}"] \arrow[d, "\beta"] & (J_n/p^N)_\chi \arrow[d, "\alpha"] \\
R_N^h \arrow[r, "\bar{f}"] & R_N^h \, .
\end{tikzcd}$$

7.2. Let δ be a non-zero element of $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin}})$. In this and the next subsection, we write $\bar{\phi}^\ell$ in place of $\bar{\phi}^\ell_{F,N,\chi}$ for simplicity. Here, as in [Ku], we shall take the element $x_{\nu,q} \in (F^\times/p^N)_\chi$ which is defined in Definition 4.16, to translate β_r to homomorphisms of the type $\bar{\phi}^\ell$. Recall the element $x_{\nu,q} \in (F^\times/p^N)_\chi$ is determined by q, ν, and $\{a_\ell\}_{\ell \mid \nu}$. We shall take them as follows.

First, we take a prime number q by the following way. For each integer r with $1 \leq r \leq h$, we fix a prime number $q_r \in P_{n_r}$. We put $Q := \prod_{r=1}^h q_r \in \mathcal{N}_N$. By the Iwasawa main conjecture, we can take an isomorphism

$$\varphi \colon (\overline{\mathcal{O}_\infty^1})_\chi \xrightarrow{\simeq} \Lambda_\chi$$

which sends $\big(u \cdot \mathrm{cyc}(\rho_m)_\chi\big)_{m \geq 0}$ to $\det M_0$. Let

$$\bar{\varphi}_{F,N,\chi} \colon \big(N_\infty(\mathcal{O}_F^1)/p^N\big)_\chi \xrightarrow{\simeq} R_N$$

be the induced isomorphism by φ. Recall that we define $\mathcal{NO}_{F_m,N,\chi}$ to be the image of the natural homomorphism

$$\big(N_\infty(\mathcal{O}_{F_m}^\times)/p^N\big)_\chi \longrightarrow \big(\mathcal{O}_{F_m}^\times/p^N\big)_\chi \subset \big(F_m^\times/p^N\big)_\chi.$$

By Lemma 6.9, there exists a homomorphism $\psi \colon \mathcal{NO}_{F,N,\chi} \longrightarrow R_N$ which makes the diagram

$$\begin{tikzcd}
(C_F^1/p^N)_\chi \arrow[r] \arrow[d] & \big(N_\infty(\mathcal{O}_F^1)/p^N\big)_\chi \arrow[r, "\delta\bar{\varphi}_{F,N,\chi}"] \arrow[d] & R_N \\
W_{F_m,N,\chi}^1 \arrow[r, hook] & \mathcal{NO}_{F,N,\chi} \arrow[ur, dashed, "\psi"'] &
\end{tikzcd}$$

commute. By Proposition 5.1, we can take a prime number $q \in \mathcal{S}_N$ satisfying the following two conditions:

(q1) the class of q_{F_m} in $A_{m,\chi}$ coincides with the class of q_{1F};
(q2) $\mathcal{NO}_{F,N,\chi}$ is contained in the kernel of $[\cdot]_{F,N,\chi}^q$, and for all $x \in \mathcal{NO}_{F,N,\chi}$,

$$\psi(x) = \bar{\phi}^q(x).$$

In particular, we have

$$\begin{aligned}
\bar{\phi}^q(\mathrm{cyc}(\rho_m)) &= \bar{\phi}^q(u \cdot \mathrm{cyc}(\rho_m)) \\
&= \delta\bar{\varphi}_{F,N,\chi}(\mathrm{cyc}(\rho_m)) \\
&= \delta \det M_0.
\end{aligned}$$

We replace q_1 by q.

Next, we shall take ν and $\{a_\ell\}_{\ell \mid \nu}$.

First, we consider the homomorphism $\beta_{m_1} \colon \mathcal{F}_{Q,N} \longrightarrow R_N$. Applying Proposition 5.1, we can take $\ell_2 \in \mathcal{S}_N(F(Q))$ such that $\ell_2 \in P_{n_2}$, $\ell \neq q_2$, and

$$\beta_{m_1}(x) = \bar{\phi}^{\ell_2}(x)$$

for all $x \in \mathcal{F}_{Q,N}$. We put $\nu_1 := 1$.

In the case $i = 1$, we put $\nu := \nu_1 = 1$, and $x_{\nu,q} = x_{1,q} = \kappa_q(\xi_q)$. It follows from Proposition 4.17 (1) and Lemma 7.3 that $x_{1,q}^\delta$ is an element of $\mathcal{F}_{Q,N}$.

Suppose $i \geq 2$. To take ν and $\{a_\ell\}_{\ell \mid \nu}$, we choose prime numbers ℓ_r for each r with $2 \leq r \leq i+1$ by induction on r as follows. Let r be an integer satisfying $2 < r \leq i+1$, and suppose that we have chosen distinct prime numbers $\ell_s \in \mathcal{S}_N(F(Q\nu_{s-1}))$ for each s with $2 \leq s \leq r-1$. We put $\nu_{r-1} := \prod_{s=2}^{r-1} \ell_s$. We consider the homomorphism $\beta_{m_1} \colon \mathcal{F}_{Q\nu_{r-1},N} \longrightarrow R_N$. Applying Proposition 5.1, we can take $\ell_r \in \mathcal{S}_N(F(Q\nu_{r-1}))$ satisfying the following conditions:

(x1) $\ell_r \in P_{n_r}$, and $\ell \neq q_r$;
(x2) there exists $b_r \in (F^\times \otimes \mathbb{Z}_p)_\chi$ such that $(b_r)_{F,\chi} = (\ell_{r,F} - q_{r,F})_\chi$ and $\bar{\phi}^{\ell_s}(b_r) = 0$ for any s with $2 \leq s < r$;
(x3) $\bar{\phi}^{\ell_r}(x) = \beta_{m_{r-1}}(x)$ for any $x \in \mathcal{F}_{Q\nu_{r-1},N}$.

Thus, we have taken $\ell_2, \ldots, \ell_{i+1}$, and we put $\nu := \nu_i = \prod_{r=2}^{i} \ell_r \in \mathcal{N}_N$. For each r with $2 \leq r \leq i$, we put $a_{\ell_r} := -\phi^{\ell_r}(b_r) \in R_N \otimes H_{\ell_r}$, and we obtain $x_{\nu,q} \in (F^\times/p^N)_\chi$. It follows from Proposition 4.17 (1) and Lemma 7.3 that $x_{\nu,q}^\delta$ is an element of $\mathcal{F}_{Q\nu,N}$. Note that $q\nu$ is *well-ordered.*

7.3. In this subsection, we observe two homomorphism α and β by using $x_{n,q}$, and describe $\det M_i$ in R_N. First, we prepare the following lemma.

Lemma 7.5 (cf. [Ku] Lemma 9.2)**.** *Suppose $i \geq 2$. Then,*

(1) $\beta_{m_{r-1}}(x_{\nu,q}^\delta) = 0$ *for all r with $2 \leq r \leq i$;*
(2) $\alpha_j([x_{\nu,q}]_{F,\chi}) = 0$ *for any $j \neq n_1, \ldots, n_i$.*

Proof. The second assertion (2) of the above lemma is clear by Proposition 4.17 (1).

We shall prove the first assertion. For any r satisfying $2 \leq r \leq i$, we have $\alpha([b_r]_{F,\chi}) = 0$ since $(b_r)_{F,\chi} = (\ell_{r,F} - q_{r,F})_\chi$. Then, by the definition of β, we have $\beta(b_r) = 0$. We put

$$y_r = x_{\nu,q} \prod_{s=r}^{i} b_s^{\bar{\phi}^{\ell_s}(x_{\nu/\ell_s,q})},$$

then we have $\beta(x_{\nu,q}^\delta) = \beta(y_r^\delta)$. We will prove $\beta_{m_{r-1}}(y_r^\delta) = 0$ for any r satisfying $2 \leq r \leq i$.

By Proposition 4.17 (2), we have $[y_r]_{F,N,\chi} \in J_{Q\nu_{r-1}}$, and then, by Lemma 7.3, we have $y_r^\delta \in \mathcal{F}_{Q\nu_{r-1},N}$. Therefore, we obtain

$$\delta\bar{\phi}^{\ell_r}(y_r) = \beta_{m_{r-1}}(y_r^\delta)$$

by the condition (x3). Since $\bar{\phi}^{\ell_r}(b_s) = 0$ for all integers s satisfying $r+1 \leq s \leq i$ by the condition (x2), we have

$$\bar{\phi}^{\ell_r}(y_r) = \bar{\phi}^{\ell_r}(x_{\nu,q} b_r^{\bar{\phi}^{\ell_r}(x_{\nu/\ell_r,q})}).$$

By Proposition 4.17 (3), we have

$$\bar{\phi}^{\ell_r}(x_{\nu,q} b_r^{\bar{\phi}^{\ell_r}(x_{\nu/\ell_r,q})}) = -\bar{\phi}^{\ell_r}(b_r)\bar{\phi}^{\ell_r}(x_{\nu/\ell_r,q}) + \bar{\phi}^{\ell_r}(x_{\nu/\ell_r,q})\bar{\phi}^{\ell_r}(b_r) = 0.$$

Therefore, we obtain $\beta_{m_{r-1}}(x_{\nu,q}^\delta) = \beta_{m_{r-1}}(y_r^\delta) = 0$. □

The goal of this subsection is the following proposition.

Proposition 7.6 (cf. [Ku] p.44)**.** *We have the following equalities on elements of R_N:*

(1) $\delta(\det M)\bar{\phi}^{\ell_2}(x_{1,q}) = \pm\delta^2(\det M_1)\bar{\varphi}_{F,N,\chi}(\mathrm{cyc}(\rho_m)_\chi)$;
(2) $\delta(\det M_{r-1})\bar{\phi}^{\ell_{r+1}}(x_{\nu_r,q}) = \pm\delta(\det M_r)\bar{\phi}^{\ell_r}(x_{\nu_{r-1},q})$ *for any r with $2 \leq r \leq i$,*

where the signs ± in (1) and (2) do not depend on m.

Proof. For each r satisfying $1 \leq r \leq i$ we put

$$\mathbf{x}^{(r)} := \beta(x^{\delta}_{\nu_r,q}) \in R^h_N \quad \text{and} \quad \mathbf{y}^{(r)} := \alpha(x^{\delta}_{\nu_r,q}) \in R^h_N,$$

and regard them as column vectors. Then, we have $\mathbf{y}^{(r)} = M\mathbf{x}^{(r)}$ in R^h_N.

We first prove the assertion (1) of the above proposition. Since $x^{\delta}_{1,q}$ is an element of $\mathcal{F}_{q,N}$, we have

$$\begin{aligned}\mathbf{y}^{(1)} &= \delta[\kappa_q(\xi_q)_\chi]^q_{F,N,\chi}\mathbf{e}^{(m)}_{n_1} \\ &= -\delta\bar{\phi}^q(\mathrm{cyc}(\rho_m)_\chi)\mathbf{e}^{(m)}_{n_1} && \text{(by Proposition 4.12 (2))} \\ &= -\delta^2\bar{\varphi}_{F,N,\chi}(\mathrm{cyc}(\rho_m)_\chi)\mathbf{e}^{(m)}_{n_1} && \text{(by condition (q2)).}\end{aligned}$$

Let $\widetilde{M}$ be the matrix of cofactors of M. Multiplying the both sides of $\mathbf{y}^{(1)} = M\mathbf{x}^{(1)}$ by $\widetilde{M}$, and comparing the m_1-st components, we obtain

$$(-1)^{n_1+m_1+1}(\det M_1)\delta^2\bar{\varphi}_{F,N,\chi}(\mathrm{cyc}(\rho_m)_\chi) = (\det M)\beta_{m_1}(x^{\delta}_{1,q}).$$

By condition (x3) for ℓ_2, we have $\beta_{m_1}(x^{\delta}_{1,q}) = \delta\bar{\phi}^{\ell_2}(x_{1,q})$, and the assertion (1) follows.

Next, we assume $i \geq 2$, and we shall prove Proposition 7.6 (2). The proof is essentially the same as the proof of assertion (1). It is sufficient to prove the assertion when $r = i$. We write $\mathbf{x} = \mathbf{x}^{(i)}$ and $\mathbf{y} = \mathbf{y}^{(i)}$. Let $\mathbf{x}' \in R^{h-i+1}_N$ be the vector obtained from $\mathbf{x}$ by eliminating the m_j-th rows for $j = 1, ..., i-1$, and $\mathbf{y}'$ the vector obtained from $\mathbf{y}$ by eliminating the n_k-th rows for $k = 1, ..., i-1$. Since the m_r-th rows of $\mathbf{x}$ are 0 for all r with $1 \leq r \leq i-1$ by Lemma 7.5 (1), we have $\mathbf{y}' = M_{i-1}\mathbf{x}'$. We assume the m'_i-th component of $\mathbf{x}'$ corresponds to the m_i-th component of $\mathbf{x}$, and the n'_i-th component of $\mathbf{y}'$ corresponds to the n_i-th component of $\mathbf{y}$. By Lemma 7.5 (2) and Proposition 4.17 (2), we have

$$\mathbf{y}' = -\delta\bar{\phi}^{\ell_i}(x_{\nu_{i-1},q})\mathbf{e}'^{(m)}_{n'_i},$$

where $(\mathbf{e}'^{(m)}_i)^{h-i+1}_{i=1}$ denotes the standard basis of R^{h-i+1}_N.

Let $\widetilde{M_{i-1}}$ be the matrix of cofactors of M_{i-1}. Multiplying the both sides of $\mathbf{y}' = M_{i-1}\mathbf{x}'$ by $\widetilde{M_{i-1}}$, and comparing the m'_i-th components, we obtain

$$(-1)^{n'_i+m'_i+1}(\det M_i)\delta\bar{\phi}^{\ell_i}(x_{\nu_{i-1},q}) = (\det M_{i-1})\beta_{m_i}(x^{\delta}_{\nu,q}).$$

By condition (x3) for ℓ_{i+1}, and since $x^{\delta}_{n,q}$ is an element of $\mathcal{F}_{Q\nu,N}$, we have

$$\beta_{m_i}(x^{\delta}_{\nu,q}) = \delta\bar{\phi}^{\ell_{i+1}}(x_{\nu,q}).$$

Here, the proof of Proposition 7.6 is complete. □

7.4. Now we prove Theorem 1.1.

Proof of Theorem 1.1 . We may vary m in the proof of Theorem 1.1. So, the element $\bar{\phi}^{\ell_{r+1}}(x_{\nu_r,q}) \in R_N = (\mathbb{Z}/p^{N_m})[\mathrm{Gal}(F_m/F_0)]_\chi$ defined in §6.2 is denoted by $\bar{\phi}^{\ell_{r+1}}(x_{\nu_r,q})_m$.

By induction on r, we shall prove that $\left(\bar{\phi}^{\ell_{r+1}}(x_{\nu_r,q})_m\right)_{m\geq 0}$ converges to $\pm\delta\det M_r \in \Lambda_\chi$, where a sequence $(a_m)_{m\geq 0} \in \prod_{m\geq 0} R_{F_m,N_m,\chi}$ is said to *converge* to $b = (b_m)_{m\geq 0} \in \varprojlim_{m\geq 0} R_{F_m,N_m,\chi} = \Lambda_\chi$ if for each m, there exists an integer L_m such that the image of $a_{m'}$ in $R_{F_m,N_m,\chi}$ coincides to $b_m \in R_{F_m,N_m,\chi}$ for any $m' \geq L_m$.

First, we consider the equality $\delta(\det M)\bar{\phi}^{\ell_2}(x_{1,q})_m = \pm\delta^2(\det M_1)\bar{\varphi}_{F,N,\chi}(\mathrm{cyc}(\rho_m)_\chi)$. Since the right hand side converges to $\pm\delta^2(\det M_1)(\det M)$ and both δ and $\det M$ are non-zero element, we find that $\left(\bar{\phi}^{\ell_2}(x_{1,q})_m\right)_{m\geq 0}$ converges to $\pm\delta\det M_1$. (Note the sign ± does not depend on m, see Proposition 7.6).

Next, we assume that $\left(\bar{\phi}^{\ell_r}(x_{\nu_{r-1},q})_m\right)$ converges to $\pm\delta\det M_{r-1}$. Then, the right hand side of $\delta(\det M_{r-1})\bar{\phi}^{\ell_{r+1}}(x_{\nu_r,q}) = \pm\delta(\det M_r)\bar{\phi}^{\ell_r}(x_{\nu_{r-1},q})$ converges to $\pm\delta^2(\det M_r)(\det M_{r-1})$. Since we take $\det M_{r-1} \neq 0$, the sequence $\left(\bar{\phi}^{\ell_{r+1}}(x_{\nu_r,q})_m\right)_{m\geq 0}$ converges to $\pm\delta\det M_r$.

By induction, we conclude $\left(\bar{\phi}^{\ell_{i+1}}(x_{\nu,q})_m\right)$ converges to $\pm\delta\det M_i$. Since $(x_{\nu,q})_m \in W^{q\nu}_{F_m,N_m}$ with $\epsilon(q\nu) = i$, we have $\bar{\phi}^{\ell_{i+1}}(x_{\nu,q})_m \in \mathfrak{C}_{i,F_m,N\chi}$ for all $m \in \mathbb{Z}_{\geq 0}$. Hence we have $\delta\det M_i \in \mathfrak{C}_{i,\chi}$. This completes the proof of Theorem 1.1. □

Remark 7.7. We remark on the higher Fitting ideals of the trivial character parts of X and X'. Let 1_Δ be the trivial character in $\widehat{\Delta}$. It is a well-known fact that $X_{1_\Delta} = 0$ (cf. [Wa] Proposition 15.43). In particular, we have

$$\mathrm{Fitt}_{\Lambda_{1_\Delta},i}(X_{1_\Delta}) = \mathrm{Fitt}_{\Lambda_{1_\Delta},i}(X'_{1_\Delta}) = \Lambda_{1_\Delta}$$

for $i \geq 0$.

7.5. Here, we remark on some application of Theorem 1.1.

For each ideal I of Λ_χ, we denote the unique minimal principal ideal of Λ_χ containing I by $\mathcal{P}(I)$. Since Λ_χ is UFD, the ideals $\mathcal{P}(I)$ are well-defined. Recall that we denote the smallest number of generators of an R-module M by $\nu_R(M)$ (cf. §3). We obtain the following corollary of Theorem 1.1.

Corollary 7.8. *Let χ be a non-trivial character in $\widehat{\Delta}$. Then,*

$$\mathrm{Fitt}_{\Lambda_\chi,i}(X_\chi) \subseteq \mathrm{Fitt}_{\Lambda_\chi,i}(X'_\chi) \subseteq \mathcal{P}(\mathfrak{C}_{i,\chi})$$

for all $i \geq 0$. In particular, if $\mathcal{P}(\mathfrak{C}_{i,\chi}) \neq \Lambda_\chi$, then we have $\nu_{\Lambda_\chi}(X_\chi) \geq i+1$ and $\nu_{\Lambda_\chi}(X'_\chi) \geq i+1$.

Proof. Since X'_χ is a quotient module of X_χ, we obtain the first inclusion

$$\mathrm{Fitt}_{\Lambda_\chi,i}(X_\chi) \subseteq \mathrm{Fitt}_{\Lambda_\chi,i}(X'_\chi).$$

The second inclusion follows from Theorem 1.1 immediately. □

Remark 7.9. Let $\chi \in \widehat{\Delta}$ be a non-trivial character. Since X_χ is pseudo-isomorphic to X'_χ, we have $\mathrm{char}_{\Lambda_\chi}(X_\chi) = \mathrm{char}_{\Lambda_\chi}(X'_\chi)$. Since $\mathrm{ann}_{\Lambda_\chi}(X_{\mathrm{fin},\chi})$ is an ideal of Λ_χ whose index is finite, we have $\mathrm{char}_{\Lambda_\chi}(X'_\chi) = \mathrm{Fitt}_{\Lambda_\chi,0}(X'_\chi) = \mathcal{P}(\mathfrak{C}_{0,\chi})$ by Lemma 3.3 and Theorem 1.1 for $i = 0$. By Proposition 6.7, we have $\mathcal{P}(\mathfrak{C}_{0,\chi}) = \mathrm{char}_{\Lambda_\chi}\left((\overline{\mathcal{O}^1_\infty}/\overline{C^1_\infty})_\chi\right)$. Hence Theorem 1.1 is a refinement of the Iwasawa main conjecture.

From Corollary 7.8, we obtain the following results on the higher Fitting ideals of $A_{m,\chi}$ and $A'_{m,\chi}$.

Corollary 7.10. *Let χ be a non-trivial character in $\widehat{\Delta}$. For each $m \geq 0$, we denote the image of $\mathcal{P}(\mathfrak{C}_{i,\chi})$ in $R_{F_m,\chi} = \mathbb{Z}_p[\mathrm{Gal}(F_m/\mathbb{Q})]_\chi$ by $\mathcal{P}(\mathfrak{C}_{i,\chi})_m$. Then,*

$$\mathrm{Fitt}_{R_{F_m,\chi},i}(A_{m,\chi}) \subseteq \mathrm{Fitt}_{R_{F_m,\chi},i}(A'_{m,\chi}) \subseteq \mathcal{P}(\mathfrak{C}_{i,\chi})_m$$

for all $m \geq 0$ and $i \geq 0$. In particular, if $\mathcal{P}(\mathfrak{C}_{i,\chi}) \neq \Lambda_\chi$, then we have $\nu_{R_{F_m,\chi}}(A_{m,\chi}) \geq i+1$ and $\nu_{\Lambda_\chi}(A'_{m,\chi}) \geq i+1$.

Remark 7.11. We can know more about $\nu_{R_{F_m,\chi}}(A_{m,\chi})$ and $\nu_{R_{F_m,\chi}}(A_{m,\chi})$ by direct application of the result in [MR] (see Remark 6.11) without using Theorem 1.1. Let $\chi \in \widehat{\Delta}$ be a non-trivial character. Suppose N is sufficiently large. By Nakayama's lemma, the following conditions are equivalent:

(1) $\dim_{\mathbb{F}_p} A_{0,\chi}/p = i+1$;
(2) $\nu_{\Lambda_\chi}(X_\chi) = i+1$;
(3) $\nu_{R_{F_m,\chi}}(A_{m,\chi}) = i+1$;
(4) $\mathrm{Fitt}_{\Lambda_\chi,i}(X_\chi) \neq \Lambda_\chi$ and $\mathrm{Fitt}_{\Lambda_\chi,i+1}(X_\chi) = \Lambda_\chi$;
(5) $\mathrm{Fitt}_{R_{F_m,\chi},i}(A_{m,\chi}) \neq R_{F_m,\chi}$ and $\mathrm{Fitt}_{R_{F_m,\chi},i+1}(A_{m,\chi}) = R_{F_m,\chi}$;
(6) $\mathfrak{C}_{i,F_m,N} \neq R_{F_m,\chi}$ and $\mathfrak{C}_{i+1,F_m,N} = R_{F_m,\chi}$.

References

[CS] Coates, J. and Sujatha, R., *Cyclotomic Fields and Zeta Values*, Springer Berlin Heidelberg (2006).

[Gr] Greenberg, R., *Iwasawa theory—past and present*, Class field theory—its centenary and prospect (Tokyo, 1998), 335–385, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

[Ku] Kurihara, M., *Refined Iwasawa theory and Kolyvagin systems of Gauss sum type*, preprint (2008).

[MR] Mazur, B., and Rubin, K., *Kolyvagin systems*, Memoirs of the AMS Vol **168**, Number **799** (2004).

[MW] Mazur, B., and Wiles, A., *Class fields of abelian extension of* **Q**, Invent. math. **76** (1984), 179-330.

[No] Northcott, D. G., *Finite free resolusions*, Cambridge Univ. press (1976).

[Ru1] Rubin, K., The main conjecture, Appendix to *Cyclotomic fields I and II* by S. Lang, Gradiate Texts in mathematics **121**, Springer-Verlag (1990), 397-419.

[Ru2] Rubin, K., *Kolyvagin's system of Gauss sums*, Arithmetic geometry, G. van der Geer et al eds, Progress in Math **89** (1991), 309-324.

[Wa] Washington, L., *Introduction to Cyclotomic Fields*, 2nd edition, Gradiate Texts in mathematics **83**, Springer-Verlag (1997).

Department of Mathematics, Kyoto University, Kyoto 606-8502, Japan

E-mail address: ohshita@math.kyoto-u.ac.jp